Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά C

C/2026/6013

17.11.2026

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

Καθοδήγηση της Επιτροπής σχετικά με την εφαρμογή του κανονισμού (ΕΕ) 2024/2847 (κανονισμός για την κυβερνοανθεκτικότητα)

(C/2026/6013)

Περιεχόμενα

Σελίδα

1. ΕΙΣΑΓΩΓΗ ... 3
   1.1. Κανονισμός για την κυβερνοανθεκτικότητα ... 3
   1.2. Σκοπός της καθοδήγησης ... 3
2. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ... 4
   2.1. Θέση σε κυκλοφορία στην αγορά ... 4
   2.2. Λογισμικό ως προϊόν με ψηφιακά στοιχεία ... 5
   2.3. Κώδικας υπολογιστή ... 6
   2.4. Συνδυασμός υλισμικού και λογισμικού που αποτελούν προϊόν με ψηφιακά στοιχεία ... 7
   2.5. Σύνδεση δεδομένων ... 8
   2.6. Σύνθετα συστήματα ... 8
   2.7. Προϊόντα με ψηφιακά στοιχεία που σχεδιάστηκαν πριν από την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα ... 9
3. ΕΛΕΥΘΕΡΟ ΛΟΓΙΣΜΙΚΟ ΑΝΟΙΚΤΟΥ ΚΩΔΙΚΑ ... 11
   3.1. Προσδιορισμός του αν το ελεύθερο λογισμικό ανοικτού κώδικα τελεί υπό την ευθύνη κάποιου ... 12
   3.2. Προσδιορισμός του αν ελεύθερο λογισμικό ανοικτού κώδικα τίθεται σε κυκλοφορία στην αγορά της ΕΕ ... 13
      3.2.1. Χρέωση ... 13
      3.2.2. Αποκόμιση οικονομικού οφέλους από άλλες υπηρεσίες ή απαίτηση επεξεργασίας δεδομένων προσωπικού χαρακτήρα ... 13
      3.2.3. Υπηρεσίες υποστήριξης ... 14
      3.2.4. Δωρεές ... 15
      3.2.5. Χρηματοδότηση ελεύθερου λογισμικού ανοικτού κώδικα ... 15
      3.2.6. Μη κερδοσκοπικές οντότητες που έχουν συσταθεί για την επίτευξη μη κερδοσκοπικών στόχων ... 16
      3.2.7. Ενσωμάτωση από άλλους κατασκευαστές ... 16
   3.3. Υποστηρικτές λογισμικού ανοικτού κώδικα ... 16
      3.3.1. Διαρκής υποστήριξη και διασφάλιση της βιωσιμότητας του ελεύθερου λογισμικού ανοικτού κώδικα ... 17
   3.4. Συνεισφέροντες και κατάντη χρήσεις ... 18
   3.5. Ενδεικτικά σενάρια ... 19
4. ΟΥΣΙΑΣΤΙΚΕΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ ΚΑΙ ΑΝΤΑΛΛΑΚΤΙΚΑ ... 21
   4.1. Υλικές επισκευές ... 22
   4.2. Ανταλλακτικά ... 23
   4.3. Ενημερώσεις λογισμικού ως ουσιώδεις τροποποιήσεις ... 24

4.4. Συνέπειες της ουσιαστικής τροποποίησης 27
4.4.1. Ουσιαστικές τροποποιήσεις που πραγματοποιούνται από πρόσωπο διαφορετικό από τον αρχικό κατασκευαστή 28
4.4.2. Ουσιαστικές τροποποιήσεις που πραγματοποιούνται από τον αρχικό κατασκευαστή 29
5. ΠΕΡΙΟΔΟΣ ΥΠΟΣΤΗΡΙΞΗΣ 29
5.1. Ουσιαστικές τροποποιήσεις και η περίοδος υποστήριξης 31
6. ΣΗΜΑΝΤΙΚΑ ΚΑΙ ΚΡΙΣΙΜΑ ΠΡΟΪΟΝΤΑ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ 32
6.1. Βασική λειτουργικότητα 33
6.2. Αξιολόγηση της συμμόρφωσης για σημαντικά και κρίσιμα προϊόντα με ψηφιακά στοιχεία 36
6.3. Συνέπειες για το τεκμήριο συμμόρφωσης 38
7. ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΩΝ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΕΝΣΩΜΑΤΩΣΗ ΠΡΟΪΟΝΤΩΝ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ ΚΑΙ ΔΟΜΟΣΤΟΙΧΕΙΩΝ 41
7.1. Σχετικά με την αξιολόγηση και την αντιμετώπιση των κινδύνων κυβερνοασφάλειας 41
7.2. Σχετικά με τον σχεδιασμό, την ανάπτυξη και την παραγωγή προϊόντων με τρόπο ώστε να εγγυώνται κατάλληλο επίπεδο κυβερνοασφάλειας βάσει των κινδύνων. 42
7.3. Εκτίμηση κινδύνων και δέουσα επιμέλεια σε σχέση με εξωτερικές εξαρτήσεις και ενσωματωμένα δομοστοιχεία . 42
7.4. Εκ νέου χρήση εκτιμήσεων κινδύνων και εγγράφων τεκμηρίωσης της συμμόρφωσης για οικογένειες προϊόντων με ψηφιακά στοιχεία 44
8. ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ 44
8.1. Τι θεωρείται λύση εξ αποστάσεως επεξεργασίας δεδομένων για προϊόν με ψηφιακά στοιχεία; 45
8.1.1. Η έννοια «εξ αποστάσεως» 46
8.1.2. Η απουσία της εν λόγω επεξεργασίας δεδομένων θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του; 46
8.1.3. Το λογισμικό έχει σχεδιαστεί και αναπτυχθεί από τον κατασκευαστή ή υπό την ευθύνη του; 47
8.2. Πρακτικές και τεχνικές επιπτώσεις των λύσεων εξ αποστάσεως επεξεργασίας δεδομένων και εξάρτηση από λύσεις τρίτων 49
8.3. Περιπτώσεις χρήσης για λύσεις εξ αποστάσεως επεξεργασίας δεδομένων 50
8.3.1. Εφαρμογή κινητής τραπεζικής 51
8.3.2. Έξυπνος θερμοστάτης 52
8.3.3. Συσκευή ανάγνωσης ηλεκτρονικών βιβλίων 53
8.3.4. Βιομηχανικό ρομπότ 53
8.3.5. Κυψελοειδές δίκτυο 53
9. ΠΡΟΣΘΕΤΑ ΣΤΟΙΧΕΙΑ 54
9.1. Υποχρεώσεις αναφοράς 54
9.2. Χειρισμός ευπαθειών 56
9.2.1. Αναφορά ανάντη και κοινοποίηση διορθώσεων ασφαλείας 56
9.2.2. Γνωστές εκμεταλλεύσιμες ευπάθειες 57
9.2.3. Αποτελεσματικές και τακτικές δοκιμές και αξιολογήσεις 58
9.3. Αλληλεπίδραση με άλλη νομοθεσία 59
9.3.1. Κανονισμός (ΕΕ) 2019/2144 και κανονισμός (ΕΕ) αριθ. 168/2013 59
9.3.2. Ισχύς των πιστοποιητικών εξέτασης τύπου ΕΕ (άρθρο 69 παράγραφος 1) 59

1. **ΕΙΣΑΓΩΓΗ**

1.1. **Κανονισμός για την κυβερνοανθεκτικότητα**

1. Ο κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα) ([1]) άρχισε να ισχύει στις 10 Δεκεμβρίου 2024. Σκοπός του κανονισμού είναι να ενισχυθεί η προσέγγιση της ΕΕ όσον αφορά την κυβερνοασφάλεια, να αντιμετωπιστεί σε επίπεδο Ένωσης το θέμα της κυβερνοανθεκτικότητας και να βελτιωθεί η λειτουργία της εσωτερικής αγοράς με τη θέσπιση ενιαίου νομικού πλαισίου για τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας για τη θέση σε κυκλοφορία προϊόντων με ψηφιακά στοιχεία στην αγορά της ΕΕ, καθώς και κατά τη διάρκεια του κύκλου ζωής ενός προϊόντος με ψηφιακά στοιχεία.

2. Ο κανονισμός για την κυβερνοανθεκτικότητα βασίζεται στο νέο νομοθετικό πλαίσιο (ΝΝΠ) της ΕΕ που ορίζεται στον κανονισμό (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για τον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας της αγοράς όσον αφορά την εμπορία των προϊόντων και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 339/93 του Συμβουλίου και στην απόφαση 768/2008/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για κοινό πλαίσιο εμπορίας των προϊόντων και για την κατάργηση της απόφασης 93/465/ΕΟΚ του Συμβουλίου ([2]).

3. Την εποπτεία της αγοράς και την επιβολή ασκούν οι εθνικές αρχές εποπτείας της αγοράς. Τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα καλύπτονται από τον κανονισμό (ΕΕ) 2019/1020 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιουνίου 2019, για την εποπτεία της αγοράς και τη συμμόρφωση των προϊόντων και για την τροποποίηση της οδηγίας 2004/42/ΕΚ και των κανονισμών (ΕΚ) αριθ. 765/2008 και (ΕΕ) αριθ. 305/2011. Η Επιτροπή και ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) στηρίζουν τους οικονομικούς φορείς και τα κράτη μέλη στην εφαρμογή του κανονισμού για την κυβερνοανθεκτικότητα.

1.2. **Σκοπός της καθοδήγησης**

4. Δυνάμει του άρθρου 26 παράγραφος 1 του κανονισμού για την κυβερνοανθεκτικότητα η Επιτροπή υποχρεούται να δημοσιεύει καθοδήγηση για να βοηθήσει τους οικονομικούς φορείς στην εφαρμογή του κανονισμού, με ιδιαίτερη έμφαση στη διευκόλυνση της συμμόρφωσης των πολύ μικρών και των μικρών και μεσαίων επιχειρήσεων (ΜΜΕ). Στο άρθρο 26 παράγραφος 2 καθορίζονται οι ελάχιστες πτυχές που θα πρέπει να εξετάζονται στην καθοδήγηση. Σε αυτές περιλαμβάνονται οι εξής: i) το πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα (ιδίως λύσεις εξ αποστάσεως επεξεργασίας δεδομένων και ελεύθερο λογισμικό ανοικτού κώδικα)· ii) η έννοια των «περιόδων υποστήριξης»· iii) η αλληλεπίδραση μεταξύ του κανονισμού για την κυβερνοανθεκτικότητα και άλλων νομοθετικών πράξεων της ΕΕ· και iv) η έννοια της «ουσιαστικής τροποποίησης».

5. Στις 3 Δεκεμβρίου 2025 η Επιτροπή δημοσίευσε σειρά συχνών ερωτήσεων (Συχνές ερωτήσεις), οι οποίες έχουν ως στόχο να βοηθήσουν τους οικονομικούς φορείς να προετοιμαστούν για την εφαρμογή του κανονισμού για την κυβερνοανθεκτικότητα ([3]).

6. Σκοπός της παρούσας καθοδήγησης είναι να βοηθήσει τους οικονομικούς φορείς να συμμορφωθούν με τον κανονισμό για την κυβερνοανθεκτικότητα και να υποστηρίξει τις δραστηριότητες των αρχών εποπτείας της αγοράς, των κοινοποιουσών αρχών και των κοινοποιημένων οργανισμών, με σκοπό τη διασφάλιση της εναρμονισμένης επιβολής του κανονισμού για την κυβερνοανθεκτικότητα σε ολόκληρη την Ένωση. Σκοπός της παρούσας καθοδήγησης δεν είναι να καλύψει ολόκληρο το πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, αλλά να παράσχει διευκρινίσεις σχετικά με το σκεπτικό ορισμένων βασικών διατάξεων και τον τρόπο με τον οποίο μπορούν να εφαρμοστούν στην πράξη. Η παρούσα καθοδήγηση αφορά τον κανονισμό για την κυβερνοανθεκτικότητα και δεν εφαρμόζεται σε άλλες νομοθετικές πράξεις της ΕΕ.

([1]) ΕΕ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Το πρόγραμμα εργασίας της Επιτροπής για το 2026 προβλέπει την υποβολή μιας «ευρωπαϊκής πράξης για τα προϊόντα», με την οποία θα επικαιροποιείται το ΝΝΠ και οι κανόνες για την εποπτεία της αγοράς και την τυποποίηση: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52025DC0870.

([3]) Οι συχνές ερωτήσεις μπορούν να καταφορτωθούν μέσω του ιστοτόπου της Επιτροπής για την εφαρμογή του κανονισμού για την κυβερνοανθεκτικότητα, από την ειδική ιστοσελίδα Συχνών ερωτήσεων.

7. Κατά την κατάρτιση της παρούσας καθοδήγησης πραγματοποιήθηκαν εκτενείς διαβουλεύσεις με τους συμφεροντούχους, συμπεριλαμβανομένης της ομάδας εμπειρογνωμόνων για την κυβερνοασφάλεια προϊόντων με ψηφιακά στοιχεία ([4]) και μέσω δημόσιας διαβούλευσης που πραγματοποιήθηκε μεταξύ 3 Μαρτίου και 13 Απριλίου 2026 ([5]).

8. Η παρούσα καθοδήγηση δεν είναι δεσμευτική για τους οικονομικούς φορείς ή άλλους φορείς που υπόκεινται στον κανονισμό για την κυβερνοανθεκτικότητα. Δεσμευτική ερμηνεία του κανονισμού για την κυβερνοανθεκτικότητα μπορεί να δοθεί μόνο από το Δικαστήριο της Ευρωπαϊκής Ένωσης. Ωστόσο, στις εν λόγω κατευθυντήριες γραμμές παρουσιάζεται η ερμηνεία της Επιτροπής όσον αφορά τον κανονισμό για την κυβερνοανθεκτικότητα, με σκοπό την υποστήριξη της συμμόρφωσης και τη συμβολή στην αποτελεσματική εφαρμογή του κανονισμού. Επιπλέον, στην καθοδήγηση περιλαμβάνονται ορισμένα παραδείγματα για την επεξήγηση της εφαρμογής συγκεκριμένων διατάξεων. Ωστόσο, τα παραδείγματα αυτά δεν προορίζονται να αντικαταστήσουν την κατά περίπτωση αξιολόγηση, η οποία θα είναι πάντα αναγκαία για τη συνεκτίμηση των ιδιαιτεροτήτων κάθε μεμονωμένης περίπτωσης.

9. Σύμφωνα με το άρθρο 26 του κανονισμού για την κυβερνοανθεκτικότητα, η Επιτροπή μπορεί να εξετάσει το ενδεχόμενο έκδοσης περαιτέρω εγγράφων καθοδήγησης, συμπεριλαμβανομένης καθοδήγησης που απευθύνεται σε κατασκευαστές που υπόκεινται στον κανονισμό για την κυβερνοανθεκτικότητα και σε άλλη ενωσιακή νομοθεσία εναρμόνισης ή σε άλλες σχετικές νομοθετικές πράξεις της Ένωσης. Η εν λόγω καθοδήγηση μπορεί, για παράδειγμα, να αφορά ερωτήματα σχετικά με την αλληλεπίδραση μεταξύ του κανονισμού για την κυβερνοανθεκτικότητα και του κανονισμού (ΕΕ) 2024/1689 για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (κανονισμός για την τεχνητή νοημοσύνη), καθώς και του κανονισμού (ΕΕ) 2022/2554 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα (κανονισμός DORA).

2. **ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ**

2.1. **Θέση σε κυκλοφορία στην αγορά**

10. Ο κανονισμός για την κυβερνοανθεκτικότητα εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά της ΕΕ. Η έννοια της διάθεσης στην αγορά ορίζεται στο άρθρο 3 σημείο 22) του κανονισμού για την κυβερνοανθεκτικότητα ως «η προσφορά προϊόντος με ψηφιακά στοιχεία για διανομή ή χρήση στην ενωσιακή αγορά στο πλαίσιο εμπορικής δραστηριότητας, είτε έναντι πληρωμής είτε δωρεάν». Σύμφωνα με το άρθρο 3 σημείο 21), ένα προϊόν με ψηφιακά στοιχεία τίθεται σε κυκλοφορία στην αγορά της ΕΕ την πρώτη φορά που καθίσταται διαθέσιμο στην αγορά.

11. Η τελευταία έκδοση του «Γαλάζιου Οδηγού σχετικά με την εφαρμογή των κανόνων της ΕΕ για τα προϊόντα», που δημοσιεύτηκε το 2022 (στο εξής: Γαλάζιος Οδηγός) ([6]), παρέχει καθοδήγηση που διευκολύνει την κατανόηση των κανόνων της ΕΕ για τα προϊόντα και την ομοιόμορφη εφαρμογή τους στα διάφορα τομεακά νομικά πλαίσια που ευθυγραμμίζονται με το νέο νομοθετικό πλαίσιο, όπως η πράξη για την κυβερνοανθεκτικότητα. Στον Γαλάζιο Οδηγό αναφέρεται ότι οι έννοιες της θεσης σε κυκλοφορία στην αγορά και της διάθεσης στην αγορά πρέπει να νοούνται ως έννοιες που αφορούν «κάθε επιμέρους προϊόν, όχι κάποιον τύπο προϊόντος, είτε αυτό κατασκευάστηκε ως μεμονωμένη μονάδα είτε ως σειρά» (σημείο 2.3).

12. Για πιο «παραδοσιακά» προϊόντα με ψηφιακά στοιχεία που καλύπτονται από το ΝΝΠ, όπως υλισμικό με τη μορφή μηχανημάτων ή προϊόντων ραδιοεξοπλισμού με ψηφιακά στοιχεία, η έννοια της θέσης σε κυκλοφορία στην αγορά είναι καθιερωμένη και ο Γαλάζιος Οδηγός παρέχει περαιτέρω καθοδήγηση για να διευκρινιστεί πότε θεωρείται ότι τα εν λόγω προϊόντα τίθενται σε κυκλοφορία στην αγορά. Τα «συνοπτικά παραδείγματα» που περιλαμβάνονται στο σημείο 2.12 του Γαλάζιου Οδηγού παρέχουν περαιτέρω παραδείγματα της έννοιας της θέσης σε κυκλοφορία στην αγορά.

13. Ωστόσο, δεδομένης της φύσης των άυλων προϊόντων με ψηφιακά στοιχεία, όπως το αυτόνομο λογισμικό, απαιτείται περαιτέρω καθοδήγηση σχετικά με το πότε θεωρείται ότι τα εν λόγω προϊόντα με ψηφιακά στοιχεία τίθενται σε κυκλοφορία στην αγορά. Μόλις ολοκληρωθεί το στάδιο κατασκευής του λογισμικού και το προϊόν με ψηφιακά στοιχεία προσφερθεί σε υποψήφιους χρήστες στην αγορά της ΕΕ, μπορεί να θεωρηθεί ότι ο κατασκευαστής του έχει κατασκευάσει πολλαπλά αντίγραφα του ίδιου προϊόντος λογισμικού με ψηφιακά στοιχεία και τα έχει προμηθεύσει για διανομή ή χρήση. Στην πραγματικότητα, σε αντίθεση με τα υλικά προϊόντα με ψηφιακά στοιχεία, το αυτόνομο λογισμικό δεν υπόκειται σε

([4]) Ομάδα εμπειρογνωμόνων για την κυβερνοασφάλεια προϊόντων με ψηφιακά στοιχεία στο μητρώο ομάδων εμπειρογνωμόνων της Επιτροπής και άλλων παρεμφερών οργάνων.

([5]) Δημόσια διαβούλευση σχετικά με το σχέδιο καθοδήγησης της Επιτροπής σχετικά με τον κανονισμό για την κυβερνοανθεκτικότητα.

([6]) Ανακοίνωση της Επιτροπής — Ο «Γαλάζιος Οδηγός» σχετικά με την εφαρμογή των κανόνων της ΕΕ για τα προϊόντα 2022, 2022/C 247/01 (ΕΕ C 247 της 29.6.2022, σ. 1).

περιορισμούς φυσικής παραγωγής ή αποθεμάτων: κάθε πράξη διάθεσης του λογισμικού για καταφόρτωση ή διανομή έχει ως αποτέλεσμα τη δημιουργία νέου πανομοιότυπου αντιγράφου για τον χρήστη. Εφόσον αυτή η έκδοση του λογισμικού δεν τροποποιείται με τρόπο που να επηρεάζει τη συμμόρφωση με τον κανονισμό για την κυβερνοανθεκτικότητα, η θέση σε κυκλοφορία στην αγορά της ΕΕ πρέπει να θεωρείται ότι έχει πραγματοποιηθεί κατά τη στιγμή της πρώτης προσφοράς για διανομή ή χρήση. Ως εκ τούτου, η δυνατότητα μεταγενέστερης καταφόρτωσης ή διανομής της συγκεκριμένης έκδοσης του προϊόντος λογισμικού με ψηφιακά στοιχεία πρέπει να θεωρείται περίπτωση κατά την οποία το εν λόγω προϊόν λογισμικού με ψηφιακά στοιχεία διατίθεται στην αγορά ([7]).

14. Ως εκ τούτου, ένα αυτόνομο προϊόν λογισμικού με ψηφιακά στοιχεία θα πρέπει να θεωρείται ότι έχει τεθεί σε κυκλοφορία στην αγορά όταν ολοκληρωθεί το στάδιο κατασκευής του και το εν λόγω λογισμικό παρέχεται για πρώτη φορά για διανομή ή χρήση στην αγορά της ΕΕ στο πλαίσιο εμπορικής δραστηριότητας. Ο κατασκευαστής θα πρέπει να θεωρείται ότι έχει θέσει σε κυκλοφορία στην αγορά πολλαπλά αντίγραφα του ίδιου προϊόντος λογισμικού με ψηφιακά στοιχεία ταυτόχρονα. Ως εκ τούτου, ενώ πολλαπλά αντίγραφα του ίδιου λογισμικού παραμένουν μεμονωμένα προϊόντα με ψηφιακά στοιχεία, θεωρείται ότι τίθενται σε κυκλοφορία στην αγορά ταυτόχρονα, ανεξάρτητα από το πότε η κατοχή ή η χρήση κάθε μεμονωμένου αντιγράφου μεταβιβάζεται σε άλλο φυσικό ή νομικό πρόσωπο. Ταυτόχρονα, όταν ο κατασκευαστής καθιστά διαθέσιμο λογισμικό σε διαφορετικές παραλλαγές που διαφέρουν ως προς τα δομοστοιχεία, τις διαμορφώσεις ή τις ενεργοποιημένες λειτουργίες τους [για παράδειγμα, εκδόσεις (build) για διαφορετικά λειτουργικά συστήματα ή πακέτα (bundle) με διαφορετικά σύνολα χαρακτηριστικών], οι εν λόγω παραλλαγές δεν μπορούν να θεωρηθούν πολλαπλά αντίγραφα του ίδιου προϊόντος λογισμικού με ψηφιακά στοιχεία. Ως εκ τούτου, θα πρέπει να αντιμετωπίζονται ως διακριτά προϊόντα με ψηφιακά στοιχεία για τους σκοπούς της θέσης σε κυκλοφορία στην αγορά.

Παράδειγμα 1: Την 1η Ιανουαρίου 2028 η εταιρεία Α παρέχει για πρώτη φορά προς διανομή μέσω του ιστοτόπου της την έκδοση 1.0.0 του λογισμικού της Χ. Την ίδια ημέρα ο πελάτης 1 αγοράζει αντίγραφο της έκδοσης 1.0.0 του λογισμικού Χ. Στις 15 Ιανουαρίου 2028 ο πελάτης 2 αγοράζει αντίγραφο της έκδοσης 1.0.0 του λογισμικού Χ. Και τα δύο αντίγραφα της έκδοσης 1.0.0 του λογισμικού Χ τίθενται σε κυκλοφορία στην αγορά την 1η Ιανουαρίου 2028.

15. Δεδομένου του επαναληπτικού χαρακτήρα της ανάπτυξης λογισμικού, θα πρέπει να διευκρινιστεί περαιτέρω ότι οι μεταγενέστερες επαναλήψεις ενός προϊόντος λογισμικού με ψηφιακά στοιχεία θεωρούνται ως νέα θέση σε κυκλοφορία στην αγορά όταν οι εν λόγω επαναλήψεις χαρακτηρίζονται ως «ουσιαστική τροποποίηση» προϊόντος λογισμικού με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά, όπως αναφέρεται στην αιτιολογική σκέψη 41 του κανονισμού για την κυβερνοανθεκτικότητα. Ως προς τις επαναλήψεις που δεν χαρακτηρίζονται ως ουσιαστικές τροποποιήσεις, δεν απαιτείται από τον κατασκευαστή να διεξαγάγει νέα διαδικασία αξιολόγησης της συμμόρφωσης και, ως εκ τούτου, η ημερομηνία θέσης σε κυκλοφορία του εν λόγω λογισμικού στην αγορά δεν μεταβάλλεται. Για περισσότερες οδηγίες σχετικά με την έννοια των ουσιαστικών τροποποιήσεων, βλ. τμήμα *4 Substantial modifications*.

Παράδειγμα 2: Την 1η Ιανουαρίου 2028 η εταιρεία Α παρέχει για πρώτη φορά προς διανομή μέσω του ιστοτόπου της την έκδοση 1.0.0 του λογισμικού Χ. Την ίδια ημέρα ο πελάτης 1 αγοράζει αντίγραφο της έκδοσης 1.0.0 του λογισμικού Χ. Στις 15 Ιανουαρίου 2028 η εταιρεία Α εκδίδει επικαιροποιημένη έκδοση 1.0.1 του λογισμικού Χ, η οποία δεν συνιστά ουσιαστική τροποποίηση. Στις 30 Ιανουαρίου 2028 ο πελάτης 2 αγοράζει αντίγραφο της έκδοσης 1.0.1 του λογισμικού Χ. Και τα δύο αντίγραφα των εκδόσεων 1.0.0 και 1.0.1 του λογισμικού Χ θεωρείται ότι τέθηκαν σε κυκλοφορία στην αγορά την 1η Ιανουαρίου 2028.

16. Η καθοδήγηση που δίνεται στα σημεία 13, 14 και 15 εφαρμόζεται αποκλειστικά στον βαθμό που το προϊόν με ψηφιακά στοιχεία είναι αυτόνομο λογισμικό. Αυτό δεν ισχύει, για παράδειγμα, όταν το λογισμικό συνδυάζεται με υλισμικό, όπως αναλύεται στο τμήμα *2.4 Combination of hardware and software forming a product*.

2.2. **Λογισμικό ως προϊόν με ψηφιακά στοιχεία**

17. Στο άρθρο 3 σημείο 1) του κανονισμού για την κυβερνοανθεκτικότητα ως προϊόν με ψηφιακά στοιχεία ορίζεται «κάθε προϊόν λογισμικού ή υλισμικού και οι οικείες λύσεις εξ αποστάσεως επεξεργασίας δεδομένων, συμπεριλαμβανομένων των δομοστοιχείων λογισμικού ή υλισμικού που τίθενται σε κυκλοφορία στην αγορά χωριστά». Τα εν λόγω προϊόντα με ψηφιακά στοιχεία εμπίπτουν στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα όταν ο προβλεπόμενος σκοπός ή η ευλόγως προβλέψιμη χρήση τους περιλαμβάνει άμεση ή έμμεση λογική ή φυσική σύνδεση δεδομένων με συσκευή ή δίκτυο.

([7]) Σύμφωνα με το άρθρο 13 παράγραφος 11, οι κατασκευαστές μπορούν να διατηρούν δημόσια αρχεία λογισμικού που ενισχύουν την πρόσβαση των χρηστών σε ιστορικές εκδόσεις. Στις περιπτώσεις αυτές, οι χρήστες ενημερώνονται σαφώς και με εύκολα προσβάσιμο τρόπο σχετικά με τους κινδύνους που συνδέονται με τη χρήση μη υποστηριζόμενου λογισμικού.

18. Ως εκ τούτου, ο κανονισμός για την κυβερνοανθεκτικότητα μπορεί να καλύπτει σειρά προϊόντων με ψηφιακά στοιχεία, όπως: i) αυτόνομο λογισμικό, όπως εφαρμογές και προγράμματα υπολογιστών, είτε ψηφιακά είτε φυσικά διανεμόμενο· ii) υλισμικό με ενσωματωμένο λογισμικό (π.χ. συσκευές διαδικτύου των πραγμάτων, φορητοί υπολογιστές, ταμπλέτες)· iii) αυτόνομο υλισμικό (π.χ. ολοκληρωμένα κυκλώματα, μητρικές κάρτες)· και iv) κάθε συνδυασμό υλισμικού και λογισμικού που παρέχονται χωριστά αλλά προορίζονται να λειτουργούν μαζί.

19. Ως εκ τούτου, το αυτόνομο λογισμικό εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, όταν τίθεται σε κυκλοφορία στην αγορά ως προϊόν με ψηφιακά στοιχεία. Είναι χρήσιμο να γίνεται διάκριση μεταξύ των προϊόντων λογισμικού με ψηφιακά στοιχεία που υπόκεινται στον κανονισμό για την κυβερνοανθεκτικότητα και της εξ αποστάσεως παροχής υπηρεσιών που δεν εμπίπτουν στο πεδίο εφαρμογής του εν λόγω κανονισμού.

20. Για να εμπίπτει το λογισμικό στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, ένα προϊόν λογισμικού με ψηφιακά στοιχεία πρέπει να παρέχεται σε χρήστη, να αποκτάται από τον εν λόγω χρήστη και να λειτουργεί σε ηλεκτρονικό σύστημα πληροφοριών ή ως μέρος αυτού από την πλευρά του χρήστη. Το λογισμικό που καταφορτώνεται, εγκαθίσταται ή παρέχεται με άλλον τρόπο στον χρήστη και το οποίο εκτελείται στο ηλεκτρονικό σύστημα πληροφοριών του χρήστη πληροί τα εν λόγω κριτήρια, μεταξύ άλλων, για παράδειγμα, όταν λαμβάνει τη μορφή επέκτασης προγράμματος περιήγησης ή εφαρμογής που αναπτύσσεται με τη χρήση διαδικτυακών τεχνολογιών, αλλά παρέχεται για τοπική εκτέλεση.

21. Αντιθέτως, το λογισμικό που εκτελείται εξ αποστάσεως και στο οποίο έχει απλώς πρόσβαση ο χρήστης δεν αποτελεί, εξ αυτού και μόνο του λόγου, προϊόν με ψηφιακά στοιχεία. Οι αιτιολογικές σκέψεις 11 και 12 του κανονισμού για την κυβερνοανθεκτικότητα πράγματι προβαίνουν σε αυτήν τη διάκριση, καθώς διευκρινίζεται ότι η εξ αποστάσεως επεξεργασία ή αποθήκευση υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα μόνο στον βαθμό που είναι αναγκαίο για την εκτέλεση των λειτουργιών ενός προϊόντος με ψηφιακά στοιχεία [δηλαδή μέσω της έννοιας της εξ αποστάσεως επεξεργασίας δεδομένων, όπως ορίζεται στο άρθρο 3 σημείο 2)] και όχι θεωρούμενη η ίδια ως προϊόν με ψηφιακά στοιχεία. Τα ανωτέρω ισχύουν συνήθως για τις διαδικτυακές εφαρμογές, συμπεριλαμβανομένων των προοδευτικών διαδικτυακών εφαρμογών, στις οποίες η πρόσβαση γίνεται αποκλειστικά μέσω προγράμματος περιήγησης. Το ίδιο ισχύει και για τους ιστοτόπους: ενώ οι ιστότοποι μπορούν, σε περιορισμένο βαθμό, να λειτουργούν και να εκτελούνται τεχνικά στη συσκευή του χρήστη, από την αιτιολογική σκέψη 12 του κανονισμού για την κυβερνοανθεκτικότητα προκύπτει ότι οι ίδιοι οι ιστότοποι δεν πρέπει να θεωρούνται προϊόντα με ψηφιακά στοιχεία, και εμπίπτουν στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα μόνο όταν υποστηρίζουν τη λειτουργικότητα ενός προϊόντος με ψηφιακά στοιχεία, δηλαδή στον βαθμό που χαρακτηρίζονται ως εξ αποστάσεως επεξεργασία δεδομένων (όπως εξηγείται περαιτέρω στο τμήμα *8* και ιδίως στο σημείο *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its functions?*).

Παράδειγμα 3: μια εφαρμογή για φορητές συσκευές την οποία ένας χρήστης καταφορτώνει από κατάστημα εφαρμογών και εγκαθιστά στο έξυπνο τηλέφωνό του παρέχεται στον χρήστη και εκτελείται στη συσκευή του χρήστη και, ως εκ τούτου, αποτελεί προϊόν με ψηφιακά στοιχεία. Όταν τίθεται σε κυκλοφορία στην αγορά στο πλαίσιο εμπορικής δραστηριότητας, μπορεί να εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα.

Παράδειγμα 4: μια επιτραπέζια εφαρμογή που κατασκευάζεται με τη χρήση διαδικτυακών τεχνολογιών αλλά συσκευάζεται για τοπική εγκατάσταση παρέχεται στον χρήστη και εκτελείται στη συσκευή του χρήστη και, ως εκ τούτου, είναι προϊόν με ψηφιακά στοιχεία. Όταν τίθεται σε κυκλοφορία στην αγορά στο πλαίσιο εμπορικής δραστηριότητας, μπορεί να εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα.

Παράδειγμα 5: η διαδικτυακή εφαρμογή στην οποία ο χρήστης έχει πρόσβαση αποκλειστικά μέσω προγράμματος περιήγησης δεν είναι προϊόν με ψηφιακά στοιχεία. Εκτός εάν υποστηρίζει τη λειτουργικότητα ενός προϊόντος με ψηφιακά στοιχεία, δεν εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Αντιθέτως, μια εφαρμογή που παρέχεται στον χρήστη ως τοπικά εγκατεστημένο πρόγραμμα-πελάτης και εκτελείται στη συσκευή του χρήστη είναι προϊόν με ψηφιακά στοιχεία. Όταν τίθεται σε κυκλοφορία στην αγορά στο πλαίσιο εμπορικής δραστηριότητας, μπορεί να εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα.

Εάν το εν λόγω πρόγραμμα-πελάτης βασίζεται, προκειμένου να εκτελέσει μία ή περισσότερες από τις λειτουργίες του, σε εξ αποστάσεως επεξεργασία δεδομένων η οποία πληροί τον ορισμό της εξ αποστάσεως επεξεργασίας δεδομένων, η εν λόγω εξ αποστάσεως επεξεργασία δεδομένων αποτελεί επίσης μέρος του προϊόντος με ψηφιακά στοιχεία.

Παράδειγμα 6: ένας ιστότοπος που απλώς παρουσιάζει πληροφορίες στους επισκέπτες του και δεν υποστηρίζει τη λειτουργικότητα προϊόντος με ψηφιακά στοιχεία δεν είναι ο ίδιος προϊόν με ψηφιακά στοιχεία. Ως εκ τούτου, δεν εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα.

2.3. **Κώδικας υπολογιστή**

22. Είναι επίσης χρήσιμο να διευκρινιστεί αν ο πηγαίος κώδικας μπορεί να αποτελέσει προϊόν λογισμικού με ψηφιακά στοιχεία. Στον κανονισμό για την κυβερνοανθεκτικότητα το λογισμικό ορίζεται ως «το μέρος ηλεκτρονικού συστήματος πληροφοριών που αποτελείται από κώδικα υπολογιστή» [άρθρο 3 σημείο 4)]. Ο κώδικας υπολογιστή μπορεί να λάβει τη μορφή i) κώδικα μηχανής, ο οποίος είναι το σύνολο εντολών που εκτελούνται απευθείας από τον επεξεργαστή του υπολογιστή και είναι γραμμένες σε δυαδικό μορφότυπο· ή ii) πηγαίου κώδικα, ο οποίος είναι το σύνολο των εντολών και των προτάσεων που έχουν συνταχθεί σε γλώσσα προγραμματισμού, το οποίο πρέπει να μεταγλωττίζεται ή να ερμηνεύεται ώστε να εκτελείται από υπολογιστή. Ο ορισμός του λογισμικού που περιλαμβάνεται στον κανονισμό για την κυβερνοανθεκτικότητα καλύπτει και τα δύο.

23. Ένα διαφορετικό ζήτημα είναι αν μια δεδομένη παροχή κώδικα υπολογιστή ισοδυναμεί με θέση προϊόντος με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά της ΕΕ, για την οποία απαιτείται το προϊόν να παρέχεται στο πλαίσιο εμπορικής δραστηριότητας. Αυτό μπορεί συχνά να μην ισχύει για τον πηγαίο κώδικα. Για παράδειγμα, φυσικό ή νομικό πρόσωπο που διανέμει ελεύθερο ανοικτό κώδικα υπολογιστή σε δημόσια προσβάσιμα αποθετήρια δεν θεωρείται γενικά ότι θέτει τον εν λόγω κώδικα σε κυκλοφορία στην αγορά της ΕΕ για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα (όπως αναλύεται λεπτομερέστερα στο τμήμα *3 Free and open-source software*). Ο ημιτελής κώδικας που διανέμεται κατά τη διάρκεια της φάσης σχεδίασης και ανάπτυξης ενός προϊόντος με ψηφιακά στοιχεία (π.χ. για δοκιμή ή αξιολόγηση) επίσης δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα, δεδομένου ότι η φάση κατασκευής του δεν έχει ολοκληρωθεί. Ομοίως, ο κώδικας δείγματος ή επίδειξης που παρέχεται στο πλαίσιο επεξηγηματικού ή εκπαιδευτικού υλικού επίσης δεν θεωρείται ότι διατίθεται στην αγορά για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα ([8]).

24. Από την άλλη πλευρά, όταν ένας κατασκευαστής παρέχει στους πελάτες του κώδικα υπολογιστή ως προϊόν με ψηφιακά στοιχεία, ο εν λόγω κώδικας θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά, ανεξάρτητα από το αν πρόκειται για κώδικα μηχανής ή πηγαίο κώδικα ([9]).

Παράδειγμα 7: Η εταιρεία Α αδειοδοτεί πηγαίο κώδικα στην εταιρεία Β για μια εξατομικεύσιμη εσωτερική πλατφόρμα και παρέχει τον εν λόγω πηγαίο κώδικα σε αρχείο κειμένου. Ακόμα και αν ο εν λόγω πηγαίος κώδικας απαιτεί περαιτέρω προσαρμογή και μεταγλώττιση από την εταιρεία Β πριν από τη χρήση του, η εταιρεία Α θέτει τον εν λόγω πηγαίο κώδικα σε κυκλοφορία στην αγορά και, ως εκ τούτου, υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα. Η εταιρεία Α δεν είναι υπεύθυνη για τη συμμόρφωση με τον κανονισμό για την κυβερνοανθεκτικότητα των μεταγενέστερων προσαρμογών και της μεταγλώττισης του εν λόγω κώδικα από την εταιρεία Β.

2.4. **Συνδυασμός υλισμικού και λογισμικού που αποτελούν προϊόν με ψηφιακά στοιχεία**

25. Το αν το λογισμικό αποτελεί μέρος προϊόντος με ψηφιακά στοιχεία δεν θα πρέπει να καθορίζεται από τον τρόπο ή τον χρόνο παράδοσης του εν λόγω λογισμικού στον χρήστη, αλλά από το αν, υπό το πρίσμα του προβλεπόμενου σκοπού και της ευλόγως προβλέψιμης χρήσης του προϊόντος, το λογισμικό είναι αναγκαίο για την εκτέλεση των προβλεπόμενων λειτουργιών του προϊόντος με ψηφιακά στοιχεία. Όταν ένα προϊόν υλισμικού με ψηφιακά στοιχεία είναι σχεδιασμένο να λειτουργεί μαζί με συγκεκριμένο λογισμικό που παρέχεται από τον ίδιο κατασκευαστή για την εκτέλεση των λειτουργιών του, το υλισμικό και το εν λόγω λογισμικό αποτελούν από κοινού το προϊόν με ψηφιακά στοιχεία. Ως εκ τούτου, το λογισμικό που είναι απαραίτητο για τη λειτουργία, τη διαμόρφωση, τον έλεγχο ή τη χρήση ενός προϊόντος με ψηφιακά στοιχεία σύμφωνα με τον προβλεπόμενο σκοπό του αποτελεί μέρος του προϊόντος με ψηφιακά στοιχεία, ακόμα και αν αποκτάται μέσω χωριστού διαύλου (π.χ. κατάστημα εφαρμογών, σύνδεσμος καταφόρτωσης ή άλλος ψηφιακός δίαυλος μετά τη θέση του προϊόντος υλισμικού με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά). Ως εκ τούτου, η θέση του σε κυκλοφορία στην αγορά πραγματοποιείται την ίδια χρονική στιγμή κατά την οποία τίθενται σε κυκλοφορία στην αγορά μονάδες των προϊόντων υλισμικού με ψηφιακά στοιχεία.

Παράδειγμα 8: Ένας εκτυπωτής δικτύου τίθεται σε κυκλοφορία στην αγορά ως προϊόν υλισμικού με ψηφιακά στοιχεία, ενώ οι οδηγοί λογισμικού που απαιτούνται για την αποστολή εργασιών εκτύπωσης, τη διαμόρφωση της συσκευής και τη διαχείριση της λειτουργίας της διατίθενται για καταφόρτωση από τον ιστότοπο του κατασκευαστή. Μολονότι ο εκτυπωτής και οι οδηγοί παρέχονται μέσω διαφορετικών διαύλων, αποτελούν από κοινού ένα ενιαίο προϊόν με ψηφιακά στοιχεία, διότι ο εκτυπωτής δεν μπορεί να εκπληρώσει τον προβλεπόμενο σκοπό του χωρίς τους οδηγούς.

Παράδειγμα 9: Τίθεται σε κυκλοφορία στην αγορά φορετό προϊόν φυσικής κατάστασης για τη μέτρηση του καρδιακού ρυθμού και της δραστηριότητας του χρήστη, ενώ για την απεικόνιση των μετρήσεων, την προβολή του ιστορικού και τη διαμόρφωση της συσκευής απαιτείται εφαρμογή για έξυπνα τηλέφωνα που παρέχεται από τον κατασκευαστή. Παρότι η εφαρμογή καταφορτώνεται χωριστά μέσω καταστήματος εφαρμογών, το φορετό προϊόν και η εφαρμογή αποτελούν από κοινού ένα ενιαίο προϊόν με ψηφιακά στοιχεία, διότι έχουν σχεδιαστεί και προορίζονται να λειτουργούν από κοινού για την εξασφάλιση της λειτουργικότητας του προϊόντος με ψηφιακά στοιχεία.

([8]) Υπενθυμίζεται επίσης ότι το άρθρο 4 παράγραφος 3 επιτρέπει στους κατασκευαστές να διαθέτουν στην αγορά ημιτελές λογισμικό που δεν συμμορφώνεται με τον κανονισμό, όπως οι εκδόσεις «άλφα», οι εκδόσεις «βήτα» ή υποψήφιες εκδόσεις, με την προϋπόθεση ότι η ημιτελής έκδοση διατίθεται μόνο για το χρονικό διάστημα που απαιτείται για τη δοκιμή της και τη συλλογή παρατηρήσεων.

([9]) Από την άλλη πλευρά, θα πρέπει να σημειωθεί ότι, για τους σκοπούς της νομοθεσίας για την ευθύνη λόγω ελαττωματικών προϊόντων, ο ίδιος ο κώδικας υπολογιστή δεν αποτελεί προϊόν και, ως εκ τούτου, οι κατασκευαστές που θέτουν τον εν λόγω κώδικα σε κυκλοφορία στην αγορά δεν μπορούν να θεωρηθούν υπεύθυνοι βάσει της οδηγίας (ΕΕ) 2024/2853 (οδηγία για την ευθύνη λόγω ελαττωματικών προϊόντων). Στην αιτιολογική σκέψη 13 της εν λόγω οδηγίας αναφέρεται ότι «[ω]στόσο, οι πληροφορίες δεν πρέπει να θεωρούνται προϊόν και, ως εκ τούτου, οι κανόνες περί ευθύνης λόγω ελαττωματικών προϊόντων δεν θα πρέπει να εφαρμόζονται στο περιεχόμενο ψηφιακών αρχείων, όπως είναι τα αρχεία πολυμέσων ή τα ηλεκτρονικά βιβλία ή μόνο ο πηγαίος κώδικας λογισμικού». Αυτό δεν αποκλείει το ενδεχόμενο οι κατασκευαστές να υπέχουν ευθύνη βάσει του εθνικού δικαίου περί αδικοπραξιών.

2.5. **Σύνδεση δεδομένων**

26. Στο άρθρο 2 παράγραφος 1 αναφέρεται ότι ο κανονισμός για την κυβερνοανθεκτικότητα εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά των οποίων ο προβλεπόμενος σκοπός ή η ευλόγως προβλέψιμη χρήση περιλαμβάνει άμεση ή έμμεση λογική ή φυσική σύνδεση δεδομένων με συσκευή ή δίκτυο. Ως εκ τούτου, το πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα δεν βασίζεται απλώς στην παρουσία ηλεκτρονικών στοιχείων, αλλά στην ικανότητα ενός προϊόντος με ψηφιακά στοιχεία να ανταλλάσσει ψηφιακές πληροφορίες.

27. Ενώ οι όροι «λογική σύνδεση» και «φυσική σύνδεση» ορίζονται στο άρθρο 3, ο κανονισμός για την κυβερνοανθεκτικότητα δεν ορίζει τη «σύνδεση δεδομένων» ή τα «ψηφιακά δεδομένα». Ως εκ τούτου, είναι χρήσιμο να δοθεί μια ερμηνεία του τι είναι η σύνδεση δεδομένων, προκειμένου να αποσαφηνιστούν τα όρια του πεδίου εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Τα όρια αυτά είναι ιδιαίτερα σημαντικά για τη διάκριση των προϊόντων με ψηφιακά στοιχεία που χρησιμοποιούν απλώς ηλεκτρικά σήματα από εκείνα που συμμετέχουν στην ψηφιακή επικοινωνία και, ως εκ τούτου, εκτίθενται σε κινδύνους κυβερνοασφάλειας.

28. Στο πιο βασικό επίπεδο, μια σύνδεση δεδομένων περιλαμβάνει τη διαβίβαση πληροφοριών σε δυαδικό μορφότυπο, δηλαδή ως ακολουθία των ψηφίων 0 και 1. Η απλή ενεργοποίηση και απενεργοποίηση μιας εξόδου (δηλαδή 0/1) δεν συνιστά από μόνη της σύνδεση δεδομένων, εάν οι καταστάσεις αυτές δεν προορίζονται να αναπαριστούν δεδομένα ή δεν διαβάζονται από ψηφιακή είσοδο. Για να υπάρχει σύνδεση δεδομένων, οι δυαδικές καταστάσεις πρέπει να κωδικοποιούνται σκόπιμα ως πληροφορίες από μια πηγή και πρέπει να μπορούν να αποκωδικοποιούνται ως πληροφορίες στον προορισμό. Με άλλα λόγια, πρέπει να υπάρχει αποστολέας που δημιουργεί σκοπίμως ψηφιακά σύμβολα σύμφωνα με καθορισμένο σύστημα και παραλήπτης ικανός να ερμηνεύει τα σύμβολα αυτά ως δεδομένα. Όταν τα ηλεκτρικά ή ηλεκτρονικά σήματα χρησιμοποιούνται αποκλειστικά για την ενεργοποίηση ή την τροφοδότηση μιας λειτουργίας, χωρίς τη διαβίβαση ψηφιακά κωδικοποιημένων πληροφοριών, δεν υφίσταται σύνδεση δεδομένων για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα και, ως εκ τούτου, το προϊόν με ψηφιακά στοιχεία δεν εμπίπτει στο πεδίο εφαρμογής του άρθρου 2 παράγραφος 1.

2.6. **Σύνθετα συστήματα**

29. Τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα μπορεί να αποτελούνται όχι μόνο από μεμονωμένες συσκευές ή δομοστοιχεία λογισμικού, αλλά και από σύνθετα συστήματα, συμπεριλαμβανομένων συστημάτων που αποτελούνται από πολλαπλά στοιχεία υλισμικού και λογισμικού που λειτουργούν από κοινού για την εκτέλεση συγκεκριμένης λειτουργίας. Όταν ένα σύστημα αυτού του είδους τίθεται σε κυκλοφορία στην αγορά ως ενιαίο προϊόν με ψηφιακά στοιχεία, αποτελεί προϊόν με ψηφιακά στοιχεία κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα.

30. Τα εν λόγω σύνθετα συστήματα χαρακτηρίζονται συχνά από μεγάλους κύκλους σχεδιασμού και ανάπτυξης, με συμβάσεις που ενδέχεται να έχουν υπογραφεί πριν από την εφαρμογή του κανονισμού για την κυβερνοανθεκτικότητα, παρατεταμένη λειτουργική διάρκεια ζωής και υψηλό βαθμό τεχνικής και οργανωτικής πολυπλοκότητας. Τα συστήματα αυτά, τα οποία πρόκειται να τεθούν σε κυκλοφορία στην αγορά μετά την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, μπορούν να βασίζονται σε δομοστοιχεία που έχουν τεθεί σε κυκλοφορία στην αγορά πριν από την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, σε καθιερωμένες αρχιτεκτονικές ή σε ευρέως χρησιμοποιούμενα πρότυπα διαλειτουργικότητας, συμπεριλαμβανομένων των προτύπων που αναφέρονται σε άλλη νομοθεσία της ΕΕ ή ειδικά τομεακά πλαίσια. Ως εκ τούτου, ορισμένα τεχνικά χαρακτηριστικά των εν λόγω συστημάτων ενδέχεται να είναι δύσκολο ή δυσανάλογο να τροποποιηθούν χωρίς να επηρεαστεί ο προβλεπόμενος σκοπός, η ασφάλεια, η αξιοπιστία ή η διαλειτουργικότητά τους με την υφιστάμενη υποδομή.

31. Τα χαρακτηριστικά αυτά δεν αποκλείουν από μόνα τους τα σύνθετα συστήματα από το πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Αντιθέτως, αποτυπώνουν την εφαρμογή της προσέγγισης βάσει κινδύνων του κανονισμού για την κυβερνοανθεκτικότητα, η οποία επιτρέπει την απόδειξη της συμμόρφωσης με διάφορους τρόπους, ανάλογα με τα χαρακτηριστικά και τους περιορισμούς του προϊόντος με ψηφιακά στοιχεία, σύμφωνα με το άρθρο 13 παράγραφος 3 του κανονισμού για την κυβερνοανθεκτικότητα. Τα χαρακτηριστικά αυτά αποτελούν μέρος του προβλεπόμενου σκοπού και του πλαισίου λειτουργίας του και, ως εκ τούτου, είναι σημαντικά κατά την αξιολόγηση της συμμόρφωσης με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας (στο εξής: ουσιώδεις απαιτήσεις). Ειδικότερα, στην αιτιολογική σκέψη 55 αναγνωρίζεται ρητά ότι ορισμένες ουσιώδεις απαιτήσεις ενδέχεται να μην είναι πλήρως συμβατές με τη φύση ενός προϊόντος με ψηφιακά στοιχεία. Για παράδειγμα, αυτό μπορεί να συμβαίνει σε περίπτωση που η συμμόρφωση θα υπονόμευε την εκπλήρωση των υποχρεωτικών απαιτήσεων διαλειτουργικότητας ή την ορθή λειτουργία του συστήματος.

32. Ως εκ τούτου, οι κατασκευαστές υποχρεούνται να αντιμετωπίζουν τους κινδύνους κυβερνοασφάλειας με βάση την εκτίμηση των κινδύνων για την κυβερνοασφάλεια που αναφέρεται στο άρθρο 13 παράγραφος 2. Όπως εξηγείται επίσης στην αιτιολογική σκέψη 55, σε ορισμένες περιπτώσεις, ειδικές ουσιώδεις απαιτήσεις δεν εφαρμόζονται ή δεν μπορούν να

εκπληρωθούν μέσω της εφαρμογής προηγμένων μέτρων ασφάλειας λόγω, για παράδειγμα, του επιδιωκόμενου σκοπού του συστήματος, βάσει του οποίου απαιτείται το προϊόν με ψηφιακά στοιχεία να αλληλεπιδρά με υφιστάμενες εξαρτήσεις ή να τηρεί ορισμένες απαιτήσεις διαλειτουργικότητας. Στις περιπτώσεις αυτές, οι κατασκευαστές θα πρέπει να προσδιορίζουν και να τεκμηριώνουν τους εν λόγω ειδικούς περιορισμούς, να αξιολογούν τους σχετικούς κινδύνους και να εφαρμόζουν κατάλληλα εναλλακτικά ή αντισταθμιστικά μέτρα μετριασμού του κινδύνου, ώστε να μην υπονομεύεται η ασφάλεια του προϊόντος με ψηφιακά στοιχεία. Για τους σκοπούς αυτούς, τόσο ο τεχνικός φάκελος που αναφέρεται στο άρθρο 31 όσο και οι πληροφορίες και οι οδηγίες προς τον χρήστη που αναφέρονται στο παράρτημα ΙΙ διαδραματίζουν καίριο ρόλο στην περιγραφή των περιορισμών που εντοπίζονται, των σχετικών κινδύνων κυβερνοασφάλειας και των εφαρμοζόμενων μέτρων μετριασμού του κινδύνου με διαφανή τρόπο. Σύμφωνα με την υποχρέωση επικαιροποίησης της εκτίμησης κινδύνων κατά τη διάρκεια της περιόδου υποστήριξης, οι κατασκευαστές θα πρέπει επίσης να επαναξιολογούν περιοδικά το αν εξακολουθούν να υφίστανται τέτοιοι περιορισμοί. Σε περίπτωση που οι περιορισμοί αυτοί μπορούν να αρθούν ή να μειωθούν σε βάθος χρόνου, οι κατασκευαστές θα πρέπει να επικαιροποιούν αναλόγως το προϊόν με ψηφιακά στοιχεία, ώστε να μπορεί να μεταβεί προς ένα κατάλληλο επίπεδο κυβερνοασφάλειας ([10]).

Παράδειγμα 10: Ένας κατασκευαστής θέτει σε κυκλοφορία στην αγορά προϊόν με ψηφιακά στοιχεία που επικοινωνεί με εξωτερικά συστήματα μέσω πρωτοκόλλου δικτύου. Στο πλαίσιο της εφαρμογής των ουσιωδών απαιτήσεων, ο κατασκευαστής αποφασίζει, με βάση την εκτίμηση των κινδύνων για την κυβερνοασφάλεια, ότι η χρήση πρωτοκόλλου ασφαλούς επικοινωνίας είναι απαραίτητη για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων που ανταλλάσσονται από το προϊόν με ψηφιακά στοιχεία.

Ωστόσο, ο επιδιωκόμενος σκοπός του περιλαμβάνει τη διαλειτουργικότητα με υφιστάμενα συστήματα που υποστηρίζουν μόνο παλαιότερο ή λιγότερο ασφαλές πρωτόκολλο. Στις περιπτώσεις αυτές, ο κατασκευαστής μπορεί να εφαρμόσει το εν λόγω πρωτόκολλο, όταν αυτό είναι αναγκαίο για την επίτευξη διαλειτουργικότητας, υπό την προϋπόθεση ότι οι σχετικοί κίνδυνοι κυβερνοασφάλειας εντοπίζονται και μετριάζονται με άλλα μέσα.

Εφόσον είναι τεχνικά εφικτό το προϊόν με ψηφιακά στοιχεία να υποστηρίζει τόσο το ασφαλές πρωτόκολλο όσο και το λιγότερο ασφαλές πρωτόκολλο, ο κατασκευαστής αναμένεται να εφαρμόζει το ασφαλές πρωτόκολλο και να καθιστά δυνατή τη χρήση του εξ ορισμού. Η χρήση του λιγότερου ασφαλούς πρωτοκόλλου θα επιτρέπεται μόνο εφόσον απαιτείται για λόγους διαλειτουργικότητας.

Παράδειγμα 11: Ένας κατασκευαστής βιομηχανικού συστήματος αυτοματοποίησης αγοράζει ορισμένους μικροελεγκτές πριν από την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Ο κατασκευαστής διενεργεί την εκτίμηση των κινδύνων για την κυβερνοασφάλεια για το βιομηχανικό σύστημα αυτοματοποίησής του που πρόκειται να τεθεί σε κυκλοφορία στην αγορά μετά την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Με βάση την εν λόγω εκτίμηση των κινδύνων για την κυβερνοασφάλεια, ο κατασκευαστής δεν προσδιορίζει συγκεκριμένους κινδύνους για την κυβερνοασφάλεια που συνδέονται με τη χρήση ενός από τους εν λόγω μικροελεγκτές. Ο κατασκευαστής το ενσωματώνει στο βιομηχανικό σύστημα αυτοματοποίησής του και διασφαλίζει ότι το προϊόν με ψηφιακά στοιχεία στο σύνολό του (το βιομηχανικό σύστημα αυτοματοποίησης) πληροί τις ουσιώδεις απαιτήσεις.

2.7. **Προϊόντα με ψηφιακά στοιχεία που σχεδιάστηκαν πριν από την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα**

33. Σε ορισμένες περιπτώσεις, ένας κατασκευαστής θα θέτει σε κυκλοφορία στην αγορά, μετά την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα στις 11 Δεκεμβρίου 2027, μονάδες προϊόντος με ψηφιακά στοιχεία που έχουν κατασκευαστεί σύμφωνα με τύπο ή μοντέλο που έχει σχεδιαστεί και αναπτυχθεί πριν από την ημερομηνία εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Στις περιπτώσεις αυτές, για τη συμμόρφωση με τον παρόντα κανονισμό δεν απαιτείται κατ' ανάγκη ο επανασχεδιασμός των εν λόγω μονάδων του προϊόντος με ψηφιακά στοιχεία. Ο κατασκευαστής υποχρεούται να διενεργεί εκτίμηση κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 13 παράγραφος 2 του κανονισμού για την κυβερνοανθεκτικότητα, προκειμένου να προσδιορίσει, με βάση τον επιδιωκόμενο σκοπό και την ευλόγως προβλέψιμη χρήση του προϊόντος με ψηφιακά στοιχεία, ποιες από τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι μέρος Ι εφαρμόζονται στο εν λόγω προϊόν με ψηφιακά στοιχεία, καθώς και τον τρόπο εφαρμογής των εν λόγω απαιτήσεων.

34. Όταν το αποτέλεσμα της εν λόγω εκτίμησης κινδύνων καταδεικνύει ότι το προϊόν με ψηφιακά στοιχεία ενσωματώνει ήδη κατάλληλα και αποτελεσματικά μέτρα ασφάλειας για την αντιμετώπιση των σχετικών κινδύνων, ο κατασκευαστής μπορεί να βασίζεται στα εν λόγω υφιστάμενα μέτρα για να αποδείξει τη συμμόρφωση με τον κανονισμό για την κυβερνοανθεκτικότητα. Ο κανονισμός για την κυβερνοανθεκτικότητα καθ' εαυτόν δεν επιβάλλει την υποχρέωση εισαγωγής νέων χαρακτηριστικών ασφαλείας ή επανασχεδιασμού του προϊόντος με ψηφιακά στοιχεία, όταν αυτό δεν είναι αναγκαίο για την αντιμετώπιση των εντοπισθέντων κινδύνων.

([10]) Θα πρέπει να σημειωθεί ότι οι εκτιμήσεις που διατυπώνονται στην παρούσα παράγραφο μπορούν να ισχύουν, κατά περίπτωση, για όλα τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα και όχι μόνο για τα «σύνθετα συστήματα».

35. Ωστόσο, ο κατασκευαστής εξακολουθεί να υπόκειται στις υποχρεώσεις που ορίζονται στον κανονισμό για την κυβερνοανθεκτικότητα. Σε αυτές περιλαμβάνεται η διασφάλιση, πριν από τη θέση του προϊόντος με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά, ότι έχει διενεργηθεί η εφαρμοστέα διαδικασία αξιολόγησης της συμμόρφωσης, ότι έχει καταρτιστεί η δήλωση συμμόρφωσης ΕΕ και ότι έχει τοποθετηθεί η σήμανση CE. Η υποχρέωση συμμόρφωσης με τις εν λόγω απαιτήσεις είναι ανεξάρτητη από το αν απαιτούνταν τροποποίηση του σχεδιασμού του προϊόντος με ψηφιακά στοιχεία ως αποτέλεσμα της εκτίμησης κινδύνων. Όσον αφορά προϊόντα με ψηφιακά στοιχεία που σχεδιάστηκαν πριν από την ημερομηνία εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, αλλά τέθηκαν σε κυκλοφορία στην αγορά μετά την εν λόγω ημερομηνία, όταν ο κατασκευαστής δεν είναι σε θέση να αποδείξει τον τρόπο με τον οποίο ελήφθη υπόψη η εκτίμηση κινδύνων κατά το στάδιο σχεδιασμού και ανάπτυξης του προϊόντος με ψηφιακά στοιχεία, η υποχρέωση του άρθρου 13 παράγραφος 2 θα πρέπει να νοείται ως απαίτηση από τους κατασκευαστές να διενεργούν εκτίμηση κινδύνων κυβερνοασφάλειας και να αποδεικνύουν σε αυτήν τη βάση ότι το προϊόν με ψηφιακά στοιχεία ενσωματώνει επαρκή μέτρα ασφάλειας με σκοπό την ελαχιστοποίηση των κινδύνων για την κυβερνοασφάλεια, την πρόληψη περιστατικών και την ελαχιστοποίηση των επιπτώσεών τους, μεταξύ άλλων στην υγεία και την ασφάλεια των χρηστών.

36. Ως εκ τούτου, τα προϊόντα με ψηφιακά στοιχεία που έχουν σχεδιαστεί πριν από την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα μπορούν να τίθενται σε κυκλοφορία στην αγορά στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα χωρίς επανασχεδιασμό, υπό την προϋπόθεση ότι ο κατασκευαστής μπορεί να αποδείξει, μέσω της εκτίμησης κινδύνων για την κυβερνοασφάλεια και του τεχνικού φακέλου, ότι το προϊόν με ψηφιακά στοιχεία επιτυγχάνει κατάλληλο επίπεδο κυβερνοασφάλειας υπό το πρίσμα του επιδιωκόμενου σκοπού του και της ευλόγως προβλέψιμης χρήσης του και συμμορφώνεται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας.

37. Επιπλέον, είναι χρήσιμο να αποσαφηνιστεί η εφαρμογή των υποχρεώσεων αξιολόγησης της συμμόρφωσης για τους κατασκευαστές προϊόντων με ψηφιακά στοιχεία που τίθενται σε κυκλοφορία στην αγορά μετά την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, αλλά κατασκευάζονται σύμφωνα με τύπο ή μοντέλο που έχει σχεδιαστεί και αναπτυχθεί πριν από την εν λόγω ημερομηνία. Σύμφωνα με το άρθρο 13 παράγραφος 12, ο κατασκευαστής οφείλει να αποδεικνύει μέσω της σχετικής διαδικασίας αξιολόγησης της συμμόρφωσης ότι το προϊόν του με ψηφιακά στοιχεία συμμορφώνεται με τις εφαρμοστέες ουσιώδεις απαιτήσεις και να συμπεριλαμβάνει σχετικά αποδεικτικά στοιχεία στον τεχνικό φάκελο του προϊόντος (σημείο 6 του παραρτήματος VII).

38. Ωστόσο, η εφαρμογή των εν λόγω απαιτήσεων πρέπει να ερμηνεύεται υπό το πρίσμα της εκτίμησης των κινδύνων για την κυβερνοασφάλεια και του προφίλ κινδύνου για την κυβερνοασφάλεια του προϊόντος με ψηφιακά στοιχεία. Ιδίως στην περίπτωση προϊόντων με ψηφιακά στοιχεία που σχεδιάστηκαν πριν από την ημερομηνία εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα (αλλά τέθηκαν σε κυκλοφορία στην αγορά μετά την εν λόγω ημερομηνία) και υπόκεινται στις διαδικασίες αξιολόγησης της συμμόρφωσης του άρθρου 32 παράγραφος 1, όταν η εκτίμηση κινδύνων καταδεικνύει ότι το προϊόν με ψηφιακά στοιχεία ενσωματώνει ήδη κατάλληλα και αποτελεσματικά μέτρα ασφάλειας για την αντιμετώπιση των κινδύνων του εν λόγω προϊόντος, η υποχρέωση παροχής αποδεικτικών στοιχείων στο πλαίσιο της διαδικασίας αξιολόγησης της συμμόρφωσης δεν θα πρέπει να νοείται ως απαίτηση υποβολής από τον κατασκευαστή των αποτελεσμάτων των δοκιμών που καλύπτουν τα αρχικά στάδια σχεδιασμού και ανάπτυξης των εν λόγω προϊόντων με ψηφιακά στοιχεία. Αυτό δεν θα ήταν αναγκαίο, καθώς δεν θα συνέβαλε στην αύξηση της ασφάλειας του ίδιου του προϊόντος με ψηφιακά στοιχεία. Ωστόσο, σε περίπτωση που μπορεί να είναι αναγκαίες δοκιμές, οι κατασκευαστές δεν αναμένεται να παρέχουν αποδεικτικά στοιχεία των δοκιμών που διενεργούνται σε όλες τις παραλλαγές του προϊόντος, αλλά μπορούν να ομαδοποιούν τις εν λόγω δοκιμές σε οικογένειες προϊόντων με ψηφιακά στοιχεία, όπως αναλύεται περαιτέρω στο τμήμα *7.4 Reuse of risk assessments and conformity documentation for families of products with digital elements*.

39. Ωστόσο, ο κατασκευαστής θα πρέπει να παρέχει αποδεικτικά στοιχεία σχετικά με τον τρόπο με τον οποίο συμμορφώνεται με τις διαδικασίες χειρισμού των ευπαθειών που ορίζονται στο παράρτημα I μέρος II, θα πρέπει να επικαιροποιεί την εκτίμηση των κινδύνων του σύμφωνα με το άρθρο 13 παράγραφος 3, καθώς και να εκπληρώνει όλες τις άλλες υποχρεώσεις που ορίζονται στον κανονισμό για την κυβερνοανθεκτικότητα, μεταξύ άλλων παρέχοντας στους χρήστες πληροφορίες και οδηγίες σύμφωνα με το άρθρο 13 παράγραφος 18.

Παράδειγμα 12: Ένας κατασκευαστής θέτει σε κυκλοφορία στην αγορά μικροελεγκτή που σχεδιάστηκε και αναπτύχθηκε πριν από την ημερομηνία εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Ο μικροελεγκτής προορίζεται να ενσωματωθεί σε σειρά ηλεκτρονικών προϊόντων με ψηφιακά στοιχεία, συμπεριλαμβανομένων προϊόντων με ψηφιακά στοιχεία με λειτουργίες συνδεσιμότητας.

Πριν από τη θέση νέων μονάδων του μικροελεγκτή σε κυκλοφορία στην αγορά μετά την εφαρμογή του κανονισμού για την κυβερνοανθεκτικότητα, ο κατασκευαστής διενεργεί εκτίμηση κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 13 παράγραφος 2. Με βάση τον επιδιωκόμενο σκοπό του μικροελεγκτή και την ευλόγως προβλέψιμη χρήση του, ο κατασκευαστής προσδιορίζει τους σχετικούς κινδύνους για την κυβερνοασφάλεια, όπως η μη εξουσιοδοτημένη πρόσβαση, η παραποίηση λογισμικού ή δεδομένων και η κακή χρήση των διαθέσιμων διεπαφών.

Το αποτέλεσμα της εκτίμησης κινδύνων δείχνει ότι ο μικροελεγκτής, όπως σχεδιάστηκε αρχικά, ενσωματώνει ήδη κατάλληλα και αποτελεσματικά μέτρα ασφάλειας για την αντιμετώπιση των εντοπισθέντων κινδύνων. Ως εκ τούτου, ο κατασκευαστής καταλήγει στο συμπέρασμα ότι το προϊόν με ψηφιακά στοιχεία πληροί τις σχετικές ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα I μέρος I και ότι δεν απαιτείται επανασχεδιασμός ή εισαγωγή πρόσθετων λειτουργικοτήτων ασφάλειας.

Όταν δεν είναι δυνατόν να καταδειχθεί ο τρόπος με τον οποίο ελήφθη υπόψη μια εκτίμηση κινδύνων για την κυβερνοασφάλεια κατά το αρχικό στάδιο σχεδιασμού και ανάπτυξης, ο κατασκευαστής τεκμηριώνει μια τρέχουσα εκτίμηση κινδύνων για την κυβερνοασφάλεια και εξηγεί τον τρόπο με τον οποίο ο υφιστάμενος σχεδιασμός και τα υφιστάμενα μέτρα μετριάζουν τους εντοπισθέντες κινδύνους. Ο κατασκευαστής δεν υποχρεούται να αναπαραγάγει ιστορικά στοιχεία τεκμηρίωσης του σχεδιασμού ή των δοκιμών, καθώς αυτό δεν θα συμβάλει στην ενίσχυση της κυβερνοασφάλειας του προϊόντος με ψηφιακά στοιχεία. Όταν διάφορες παραλλαγές του μικροελεγκτή βασίζονται στον ίδιο σχεδιασμό και έχουν το ίδιο προφίλ κινδύνων για την κυβερνοασφάλεια, ο κατασκευαστής μπορεί επίσης να βασίζεται σε αντιπροσωπευτικά αποδεικτικά στοιχεία που καλύπτουν τη σχετική οικογένεια προϊόντων.

Ο κατασκευαστής διασφαλίζει επίσης τη συμμόρφωση με τις απαιτήσεις χειρισμού ευπαθειών που ορίζονται στο παράρτημα I μέρος II, μεταξύ άλλων με τη διατήρηση διαδικασιών για την αντιμετώπιση και τη διόρθωση ευπαθειών και με την επανεξέταση της εκτίμησης κινδύνων κυβερνοασφάλειας σύμφωνα με το άρθρο 13 παράγραφος 3.

Στις περιπτώσεις αυτές, ο μικροελεγκτής που έχει σχεδιαστεί πριν από την ημερομηνία εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα μπορεί να τίθεται σε κυκλοφορία στην αγορά χωρίς επανασχεδιασμό, υπό την προϋπόθεση ότι ο κατασκευαστής μπορεί να αποδείξει, μέσω της εκτίμησης κινδύνων κυβερνοασφάλειας και του τεχνικού φακέλου, ότι επιτυγχάνει κατάλληλο επίπεδο κυβερνοασφάλειας υπό το πρίσμα του επιδιωκόμενου σκοπού και της ευλόγως προβλέψιμης χρήσης του και ότι συμμορφώνεται με τις εφαρμοστέες ουσιώδεις απαιτήσεις.

3. **ΕΛΕΥΘΕΡΟ ΛΟΓΙΣΜΙΚΟ ΑΝΟΙΚΤΟΥ ΚΩΔΙΚΑ**

40. Όπως υπενθυμίζεται στο τμήμα *2.1 Placing on the market*, ο κανονισμός για την κυβερνοανθεκτικότητα εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά της ΕΕ στο πλαίσιο εμπορικής δραστηριότητας για πρώτη φορά (δηλαδή «τίθενται σε κυκλοφορία στην αγορά»), καθώς και σε κάθε μεταγενέστερη περίπτωση που συνιστά διάθεση του ίδιου προϊόντος με ψηφιακά στοιχεία στην αγορά. Στον Γαλάζιο Οδηγό (σημείο 2.2) διευκρινίζεται ότι ως «εμπορική δραστηριότητα» νοείται η παροχή αγαθών, έναντι αντιτίμου είτε δωρεάν, σε επιχειρηματικό πλαίσιο, και ο εμπορικός χαρακτήρας της μπορεί να εκτιμηθεί μόνο κατά περίπτωση, με γνώμονα τον τακτικό χαρακτήρα της διάθεσης, τα χαρακτηριστικά του προϊόντος, τις προθέσεις του προμηθευτή κ.λπ.

41. Η προσφορά στο πλαίσιο εμπορικής δραστηριότητας χαρακτηρίζεται από σειρά περιστάσεων, οι οποίες τεκμηριώνονται εκτενώς στον Γαλάζιο Οδηγό και υπενθυμίζονται στην αιτιολογική σκέψη 15 του κανονισμού για την κυβερνοανθεκτικότητα. Σε αυτές μπορούν να περιλαμβάνονται η άμεση χρέωση, καθώς και η «χρέωση για υπηρεσίες τεχνικής υποστήριξης, όταν αυτή δεν εξυπηρετεί μόνο την κάλυψη του πραγματικού κόστους, από την πρόθεση αποκόμισης οικονομικού οφέλους, για παράδειγμα με την παροχή πλατφόρμας λογισμικού μέσω της οποίας ο κατασκευαστής παρέχει άλλες υπηρεσίες έναντι οικονομικού οφέλους, από την απαίτηση, ως προϋπόθεση για τη χρήση, να επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα για λόγους άλλους από την αποκλειστική βελτίωση της ασφάλειας, της συμβατότητας ή της διαλειτουργικότητας του λογισμικού, ή από την αποδοχή δωρεών που υπερβαίνουν το κόστος που συνδέεται με τον σχεδιασμό, την ανάπτυξη και την παροχή προϊόντος με ψηφιακά στοιχεία» (αιτιολογική σκέψη 15) ([11]).

42. Ωστόσο, στον κανονισμό για την κυβερνοανθεκτικότητα αναγνωρίζονται οι ιδιαιτερότητες των διαφόρων τρόπων ανάπτυξης και δημοσίευσης «ελεύθερου λογισμικού ανοικτού κώδικα» (FOSS) και παρέχονται ορισμένες κατευθυντήριες γραμμές που συμβάλλουν στον προσδιορισμό του αν το ελεύθερο λογισμικό ανοικτού κώδικα αποτελεί προϊόν με ψηφιακά στοιχεία που τίθεται σε κυκλοφορία στην αγορά (δηλαδή στο πλαίσιο εμπορικής δραστηριότητας) κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα. Όπως επεξηγείται στην αιτιολογική σκέψη 18, «[α]πό μόνες τους οι συνθήκες υπό τις οποίες αναπτύχθηκε το προϊόν με ψηφιακά στοιχεία ή ο τρόπος με τον οποίο έχει χρηματοδοτηθεί η ανάπτυξη δεν θα πρέπει [...] να λαμβάνονται υπόψη κατά τον προσδιορισμό του εμπορικού ή μη εμπορικού χαρακτήρα της εν λόγω δραστηριότητας». Ειδικότερα, «προκειμένου να διασφαλιστεί ότι υπάρχει σαφής διάκριση μεταξύ των φάσεων ανάπτυξης και παροχής, η διάθεση προϊόντων με ψηφιακά στοιχεία κατατασσόμενων στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία οι κατασκευαστές τους δεν διαθέτουν έναντι οικονομικού οφέλους δεν θα πρέπει να θεωρείται εμπορική δραστηριότητα».

([11]) Υπενθυμίζεται επίσης ότι, ενώ συχνά τα προϊόντα με ψηφιακά στοιχεία αποφέρουν οικονομικό όφελος (και) μέσω της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί θεμελιώδες δικαίωμα και, ως εκ τούτου, τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να θεωρούνται εμπόρευμα, όπως αναφέρεται στην αιτιολογική σκέψη 24 της οδηγίας 2019/770 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2019, σχετικά με ορισμένες πτυχές που αφορούν τις συμβάσεις για την προμήθεια ψηφιακού περιεχομένου και ψηφιακών υπηρεσιών (ΕΕ L 136 της 22.5.2019, σ. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Επομένως, είναι χρήσιμο να i) αποσαφηνιστεί τι είναι το ελεύθερο λογισμικό ανοικτού κώδικα· ii) πότε θεωρείται ότι εμπίπτει στην ευθύνη φυσικού ή νομικού προσώπου· και iii) να παρασχεθούν παραδείγματα που θα βοηθήσουν τους συμφεροντούχους να κατανοήσουν πότε η διανομή ελεύθερου λογισμικού ανοικτού κώδικα συνιστά θέση σε κυκλοφορία στην αγορά. Όταν το ελεύθερο λογισμικό ανοικτού κώδικα δεν τίθεται σε κυκλοφορία στην αγορά, δεν εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, εκτός εάν η οντότητα που το δημοσιεύει είναι νομικό πρόσωπο που πληροί τον ορισμό του «υποστηρικτή λογισμικού ανοικτού κώδικα» (στο εξής: υποστηρικτής) σύμφωνα με το άρθρο 3 σημείο 14). Στην περίπτωση αυτήν, υπόκειται μόνο στις υποχρεώσεις που προβλέπονται στο άρθρο 24.

44. Στο άρθρο 3 σημείο 48) ως ελεύθερο λογισμικό ανοικτού κώδικα ορίζεται το «λογισμικό του οποίου ο πηγαίος κώδικας διανέμεται ανοικτά και το οποίο διατίθεται με άδεια ελεύθερης και ανοικτής πηγής η οποία περιλαμβάνει όλα τα δικαιώματα που καθιστούν το λογισμικό ελεύθερα προσβάσιμο, χρησιμοποιήσιμο, τροποποιήσιμο και αναδιανεμητέο». Μολονότι στην παρούσα καθοδήγηση δεν προσδιορίζονται συγκεκριμένες άδειες ελεύθερης και ανοικτής πηγής που είναι συμβατές με τον ορισμό του άρθρου 3 σημείο 48), από τη διατύπωση της εν λόγω διάταξης προκύπτει ότι μόνο το λογισμικό που πληροί σωρευτικά δύο προϋποθέσεις μπορεί να χαρακτηριστεί ως ελεύθερο λογισμικό ανοικτού κώδικα για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα: i) το λογισμικό πρέπει να διατίθεται βάσει άδειας ελεύθερης και ανοικτής πηγής που χορηγεί το πλήρες σύνολο των δικαιωμάτων που αναφέρονται στο άρθρο 3 σημείο 48)· και ii) ο πηγαίος κώδικας πρέπει να διανέμεται ανοικτά.

45. Η απαίτηση η άδεια να προβλέπει ότι το λογισμικό πρέπει να είναι «ελεύθερα προσβάσιμο, χρησιμοποιήσιμο, τροποποιήσιμο και αναδιανεμητέο» αντικατοπτρίζει την παραδοσιακή αντίληψη περί ελεύθερου λογισμικού ανοικτού κώδικα, δηλαδή ότι οι χρήστες πρέπει να μπορούν να έχουν πρόσβαση στον πηγαίο κώδικα, να τον χρησιμοποιούν χωρίς αδικαιολόγητους περιορισμούς, να τον τροποποιούν και να αναδιανέμουν πρωτότυπες ή τροποποιημένες εκδόσεις. Ως εκ τούτου, η πρόσβαση στον πηγαίο κώδικα αποτελεί απαραίτητη προϋπόθεση για την άσκηση των υπόλοιπων δικαιωμάτων: χωρίς πρόσβαση στον πηγαίο κώδικα, δεν είναι πρακτικά δυνατή η τροποποίηση ή η ουσιαστική επαναχρησιμοποίηση του λογισμικού.

46. Ωστόσο, το άρθρο 3 σημείο 48) δεν αναφέρεται μόνο στους όρους της άδειας, αλλά απαιτεί ρητώς «να διανέμεται ανοικτά» ο πηγαίος κώδικας. Η έννοια της «ανοικτής διανομής» υποδηλώνει ότι ο πηγαίος κώδικας πρέπει να δημοσιοποιείται (είτε «ανάντη» είτε «κατάντη») και όχι απλώς να παρέχεται σε περιορισμένη ή υπό όρους βάση. Ως εκ τούτου, το λογισμικό που διανέμεται βάσει άδειας ελεύθερης και ανοικτής πηγής, αλλά του οποίου ο πηγαίος κώδικας διανέμεται (ή επιτρέπεται να διανέμεται) μόνο σε πελάτες που πληρώνουν ή σε περιορισμένη ομάδα χρηστών, δεν πρέπει να θεωρείται ελεύθερο λογισμικό ανοικτού κώδικα κατά την έννοια του άρθρου 3 σημείο 48). Για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα, μόνο το λογισμικό του οποίου ο πηγαίος κώδικας είναι διαθέσιμος στο κοινό και αδειοδοτείται βάσει άδειας ελεύθερης και ανοικτής πηγής με την οποία χορηγείται το πλήρες σύνολο των δικαιωμάτων που αναφέρονται στο άρθρο 3 σημείο 48) θα πρέπει, ως εκ τούτου, να θεωρείται ότι μπορεί να χαρακτηριστεί ως ελεύθερο λογισμικό ανοικτού κώδικα.

3.1. **Προσδιορισμός του αν το ελεύθερο λογισμικό ανοικτού κώδικα τελεί υπό την ευθύνη κάποιου**

47. Ο κανονισμός για την κυβερνοανθεκτικότητα αποδίδει τις βασικές ευθύνες στους οικονομικούς φορείς που προμηθεύουν προϊόντα με ψηφιακά στοιχεία στην αγορά της ΕΕ. Ορίζει τον κατασκευαστή ως το φυσικό ή νομικό πρόσωπο που προμηθεύει προϊόν με ψηφιακά στοιχεία υπό τη δική του επωνυμία ή το δικό του εμπορικό σήμα στο πλαίσιο εμπορικής δραστηριότητας (θέτοντάς το έτσι σε κυκλοφορία στην αγορά). Ομοίως, εισαγωγέας είναι το φυσικό ή νομικό πρόσωπο που είναι εγκατεστημένο στην ΕΕ και προμηθεύει το προϊόν με ψηφιακά στοιχεία προσώπου εγκατεστημένου εκτός της ΕΕ στο πλαίσιο εμπορικής δραστηριότητας (θέτοντάς το έτσι σε κυκλοφορία στην αγορά). Οι υποχρεώσεις των υποστηρικτών ισχύουν για το νομικό πρόσωπο που προμηθεύει ελεύθερο λογισμικό ανοικτού κώδικα που προορίζεται για εμπορικές δραστηριότητες ([12]), αλλά δεν το θέτει σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα.

48. Ως εκ τούτου, για να προσδιοριστεί αν ένα φυσικό ή νομικό πρόσωπο θέτει ελεύθερο λογισμικό ανοικτού κώδικα σε κυκλοφορία στην αγορά της ΕΕ, πρέπει πρώτα να διευκρινιστεί αν το εν λόγω φυσικό ή νομικό πρόσωπο διαθέτει πράγματι το ελεύθερο λογισμικό ανοικτού κώδικα. Για τον ορθό προσδιορισμό των εφαρμοστέων υποχρεώσεων σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα, είναι σημαντικό να προσδιοριστεί αν το φυσικό ή νομικό πρόσωπο εκτελεί πράγματι την πράξη της προμήθειας ελεύθερου λογισμικού ανοικτού κώδικα. Στην πραγματικότητα, όπως υπενθυμίζεται στην αιτιολογική σκέψη 18, ο κανονισμός για την κυβερνοανθεκτικότητα δεν εφαρμόζεται σε φυσικά ή νομικά πρόσωπα που συνεισφέρουν πηγαίο κώδικα σε προϊόντα με ψηφιακά στοιχεία που κατατάσσονται στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία δεν τελούν υπό την ευθύνη τους.

([12]) Αυτό αποτελεί αναγκαία αλλά όχι ικανή προϋπόθεση για να χαρακτηριστεί ένα νομικό πρόσωπο ως υποστηρικτής λογισμικού ανοικτού κώδικα, καθώς ο ορισμός που παρατίθεται στο άρθρο 3 σημείο 14) προβλέπει πρόσθετες προϋποθέσεις για να χαρακτηριστεί ένα νομικό πρόσωπο ως υποστηρικτής.

49. Δεδομένων των ιδιαιτεροτήτων της ανάπτυξης του ελεύθερου λογισμικού ανοικτού κώδικα, η οποία συχνά περιλαμβάνει πολλαπλούς συνεισφέροντες, μοντέλα αποκεντρωμένης συνεργασίας και διαχωρισμό μεταξύ συνεισφοράς και λήψης αποφάσεων, είναι χρήσιμο να διευκρινιστεί ότι το ελεύθερο λογισμικό ανοικτού κώδικα θεωρείται ότι «τελεί υπό την ευθύνη» των φυσικών ή νομικών προσώπων που το δημοσιεύουν και ασκούν τον πρωταρχικό έλεγχο επί των αποφάσεων ανάπτυξης, έκδοσης και διανομής του (αναφερόμενα συχνά ως «συντηρητές»). Τα πρόσωπα που συνεισφέρουν πηγαίο κώδικα, αλλά δεν ελέγχουν τις εκδόσεις, τους χάρτες πορείας ή τις αποφάσεις διακυβέρνησης θεωρούνται «συνεισφέροντες»· στις περιπτώσεις αυτές, το ελεύθερο λογισμικό ανοικτού κώδικα δεν τελεί υπό την ευθύνη τους, παρότι συνεισέφεραν κώδικα σε αυτό. Η ύπαρξη και μόνο τεχνικών αδειών, όπως το δικαίωμα υποβολής (commit access), δεν αρκεί για να αποδειχθεί ότι το ελεύθερο λογισμικό ανοικτού κώδικα τελεί υπό την ευθύνη του εν λόγω προσώπου· την ευθύνη φέρουν όσοι δημοσιεύουν και ελέγχουν το ελεύθερο λογισμικό ανοικτού κώδικα.

Παράδειγμα 13: Μεμονωμένος προγραμματιστής ή υπάλληλος εταιρείας υποβάλλει αίτημα «ενσωμάτωσης» ή «συγχώνευσης» που περιέχει διόρθωση ασφαλείας ή νέο χαρακτηριστικό σε έργο ελεύθερου λογισμικού ανοικτού κώδικα. Οι συντηρητές του έργου επανεξετάζουν, αποδέχονται και συγχωνεύουν τον κώδικα στο κύριο αποθετήριο και, στη συνέχεια, τον συμπεριλαμβάνουν σε νέα έκδοση. Σε αυτό το σενάριο, το πρόσωπο που υπέβαλε το αίτημα ενσωμάτωσης είναι «συνεισφέρων» και δεν υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα. Μολονότι το εν λόγω πρόσωπο συνεισέφερε πηγαίο κώδικα, δεν ασκεί πρωταρχικό έλεγχο επί των αποφάσεων ανάπτυξης, έκδοσης ή διανομής.

3.2. **Προσδιορισμός του αν ελεύθερο λογισμικό ανοικτού κώδικα τίθεται σε κυκλοφορία στην αγορά της ΕΕ**

50. Μόλις διαπιστωθεί ότι ένα ελεύθερο λογισμικό ανοικτού κώδικα τελεί υπό την ευθύνη φυσικού ή νομικού προσώπου, πρέπει να διαπιστωθεί αν το εν λόγω πρόσωπο το προμηθεύει στο πλαίσιο εμπορικής δραστηριότητας, με αποτέλεσμα να συνιστά θέση σε κυκλοφορία στην αγορά.

3.2.1. *Χρέωση*

51. Όταν το φυσικό ή νομικό πρόσωπο που προμηθεύει ελεύθερο λογισμικό ανοικτού κώδικα επιβάλλει χρέωση για το ίδιο το λογισμικό (π.χ. χρεώνοντας για τα προ-μεταγλωττισμένα δυαδικά αρχεία), το εν λόγω πρόσωπο θέτει προϊόν με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά. Ως εκ τούτου, το πρόσωπο που θέτει ελεύθερο λογισμικό ανοικτού κώδικα σε κυκλοφορία στην αγορά είναι κατασκευαστής σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα.

52. Συχνά, οι κατασκευαστές ελεύθερου λογισμικού ανοικτού κώδικα προμηθεύουν δωρεάν εκδόσεις του εν λόγω λογισμικού [οι οποίες συχνά αποκαλούνται εκδόσεις «κοινότητας» (community)], των οποίων η βάση κώδικα είναι (σχεδόν) πανομοιότυπη με την επί πληρωμή έκδοση. Ωστόσο, τα εν λόγω προϊόντα με ψηφιακά στοιχεία είναι διαφορετικά προϊόντα: η επί πληρωμή έκδοση αποφέρει οικονομικό όφελος με κάποιον τρόπο (π.χ. είτε με τη χρέωση τιμήματος είτε με άλλα μέσα, όπως αναλύεται στο παρόν τμήμα) και, ως εκ τούτου, θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά, κάτι που ενεργοποιεί τις υποχρεώσεις του κατασκευαστή. Η έκδοση που παρέχεται δωρεάν (ή έκδοση κοινότητας) δεν αποφέρει οικονομικό όφελος και, ως εκ τούτου, δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα. Αυτό ισχύει επίσης όταν η επί πληρωμή έκδοση είναι «ενισχυμένη» εμπορική έκδοση, η οποία επεκτείνει τη βάση κώδικα της έκδοσης που παρέχεται δωρεάν ή ενσωματώνει την εν λόγω έκδοση σε ευρύτερο προϊόν με ψηφιακά στοιχεία (π.χ. όπως στην περίπτωση του μοντέλου «ανοικτού πυρήνα»).

53. Εάν το πρόσωπο που προμηθεύει την έκδοση κοινότητας είναι νομικό πρόσωπο, το εν λόγω νομικό πρόσωπο υπέχει επίσης τις υποχρεώσεις των υποστηρικτών για την έκδοση που προμηθεύει δωρεάν (έκδοση κοινότητας). Εάν η οντότητα είναι φυσικό πρόσωπο, η έκδοση που παρέχεται δωρεάν (η έκδοση κοινότητας) δεν εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα.

3.2.2. *Αποκόμιση οικονομικού οφέλους από άλλες υπηρεσίες ή απαίτηση επεξεργασίας δεδομένων προσωπικού χαρακτήρα*

54. Φυσικό ή νομικό πρόσωπο που δημοσιεύει ελεύθερο λογισμικό ανοικτού κώδικα μπορεί επίσης να θεωρείται ότι το θέτει σε κυκλοφορία στην αγορά (δηλαδή ότι το προμηθεύει στο πλαίσιο εμπορικής δραστηριότητας) όταν προμηθεύει το λογισμικό αποκομίζοντας μέσω αυτού οικονομικό όφελος από άλλα προϊόντα με ψηφιακά στοιχεία ή υπηρεσίες ή όταν απαιτεί ως προϋπόθεση για τη χρήση την επεξεργασία δεδομένων προσωπικού χαρακτήρα για λόγους άλλους από την αποκλειστική βελτίωση της ασφάλειας, της συμβατότητας ή της διαλειτουργικότητας του λογισμικού.

Παράδειγμα 14: Φυσικό ή νομικό πρόσωπο δημοσιεύει ελεύθερη εφαρμογή ανοικτού κώδικα με προορισμό τη διάθεσή της στην αγορά. Η εφαρμογή διατίθεται δωρεάν και επιτρέπει στους χρήστες να αγοράζουν αγαθά ή υπηρεσίες μέσω αυτής. Η εφαρμογή επιτρέπει στο πρόσωπο που τη δημοσίευσε να αποκομίζει οικονομικό όφελος από άλλα προϊόντα με ψηφιακά στοιχεία και υπηρεσίες που προσφέρονται μέσω αυτής (π.χ. μέσω διαφημίσεων, προμηθειών ή τελών συνδρομής). Ως εκ τούτου, η εφαρμογή θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά στο πλαίσιο εμπορικής δραστηριότητας.

Παράδειγμα 15: Φυσικό ή νομικό πρόσωπο δημοσιεύει ελεύθερο εικονικό ιδιωτικό δίκτυο (VPN) ανοικτού κώδικα. Η εφαρμογή διατίθεται δωρεάν, αλλά επιτρέπει στους χρήστες να πληρώνουν για να έχουν πρόσβαση σε πρόσθετους διακομιστές ή ειδικές διευθύνσεις IP. Η εφαρμογή αυτή παρέχει στο εν λόγω πρόσωπο τη δυνατότητα να αποκομίζει οικονομικό όφελος από άλλες υπηρεσίες που παρέχονται μέσω αυτής και, ως εκ τούτου, θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά στο πλαίσιο εμπορικής δραστηριότητας.

Παράδειγμα 16: Φυσικό ή νομικό πρόσωπο δημοσιεύει ελεύθερη εφαρμογή παρακολούθησης της φυσικής κατάστασης ανοικτού κώδικα. Η εφαρμογή διατίθεται δωρεάν, αλλά η χρήση της εξαρτάται από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα των χρηστών για σκοπούς όπως η στοχευμένη διαφήμιση ή η ανάλυση που δεν σχετίζονται με την ασφάλεια, τη συμβατότητα ή τη διαλειτουργικότητα του λογισμικού. Ως εκ τούτου, μέσω της απαίτησης της εν λόγω επεξεργασίας δεδομένων ως προϋπόθεσης για τη χρήση, η εφαρμογή θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά στο πλαίσιο εμπορικής δραστηριότητας.

3.2.3. *Υπηρεσίες υποστήριξης*

55. Το γεγονός και μόνο ότι ένα φυσικό ή νομικό πρόσωπο που δημοσιεύει ελεύθερο λογισμικό ανοικτού κώδικα προσφέρει επίσης συναφείς υπηρεσίες υποστήριξης επί πληρωμή δεν σημαίνει, αυτό καθαυτό, ότι το προϊόν με ψηφιακά στοιχεία παρέχεται στο πλαίσιο εμπορικής δραστηριότητας. Οι υπηρεσίες υποστήριξης μπορεί να περιλαμβάνουν δραστηριότητες όπως παροχή συμβουλών, κατάρτιση ή επαγγελματικές υπηρεσίες που σχετίζονται με τη χρήση, την τεκμηρίωση, τη διαμόρφωση και την εγκατάσταση του λογισμικού από τον πελάτη.

56. Ο καθοριστικός παράγοντας είναι αν η πρόσβαση στο ίδιο το ελεύθερο λογισμικό ανοικτού κώδικα (δηλαδή η διάθεση του προϊόντος με ψηφιακά στοιχεία), συμπεριλαμβανομένης της συντήρησής του, εξαρτάται από την καταβολή τιμήματος και όχι από την απλή προσφορά επαγγελματικών υπηρεσιών σε σχέση με ένα ελεύθερα διαθέσιμο προϊόν με ψηφιακά στοιχεία, όπως αναφέρεται στην αιτιολογική σκέψη 18 του κανονισμού για την κυβερνοανθεκτικότητα («η διάθεση προϊόντων με ψηφιακά στοιχεία κατατασσόμενων στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία οι κατασκευαστές τους δεν διαθέτουν έναντι οικονομικού οφέλους δεν θα πρέπει να θεωρείται εμπορική δραστηριότητα»). Όταν το ελεύθερο λογισμικό ανοικτού κώδικα μπορεί να καταφορτωθεί και να εγκατασταθεί ελεύθερα και οι χρήστες μπορούν προαιρετικά να επιλέξουν να αγοράσουν επαγγελματικές υπηρεσίες χωριστά, το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά.

57. Αντιθέτως, σε ορισμένες περιπτώσεις η πρόσβαση σε συγκεκριμένη έκδοση του προϊόντος με ψηφιακά στοιχεία, συμπεριλαμβανομένων ορισμένων οφελών, όπως η τεχνική βοήθεια ή η βελτιστοποίηση των επιδόσεων, εξαρτάται από την καταβολή τιμήματος. Στις περιπτώσεις αυτές, η εν λόγω διάθεση συνιστά διάθεση έναντι οικονομικού οφέλους προϊόντος με ψηφιακά στοιχεία που διατίθεται στο πλαίσιο εμπορικής δραστηριότητας και, ως εκ τούτου, θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά. Στα ανωτέρω περιλαμβάνονται περιπτώσεις στις οποίες διατίθεται επί πληρωμή έκδοση ή έκδοση για επιχειρήσεις βάσει εμπορικής συμφωνίας, ανεξάρτητα από το αν λειτουργικά ισοδύναμο λογισμικό διατίθεται επίσης δωρεάν στο πλαίσιο άδειας ελεύθερης και ανοικτής πηγής.

Παράδειγμα 17: Φυσικό ή νομικό πρόσωπο δημοσιεύει ελεύθερο λειτουργικό σύστημα ανοικτού κώδικα, προσφέροντας επί πληρωμή έκδοση του εν λόγω λειτουργικού συστήματος που περιλαμβάνει υπηρεσίες υποστήριξης, όπως τεχνική βοήθεια ή βελτιστοποίηση επιδόσεων. Η επί πληρωμή έκδοση του λειτουργικού συστήματος θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά στο πλαίσιο εμπορικής δραστηριότητας.

Παράδειγμα 18: Φυσικό ή νομικό πρόσωπο δημοσιεύει ελεύθερο εργαλείο γραμμής εντολών ανοικτού κώδικα. Το εργαλείο είναι ελεύθερα προσβάσιμο και οποιοσδήποτε μπορεί να το καταφορτώσει και να το εγκαταστήσει. Το εν λόγω φυσικό ή νομικό πρόσωπο προσφέρει χωριστά επαγγελματικές υπηρεσίες, όπως προαιρετικές συμβουλευτικές υπηρεσίες για την κατάρτιση των χρηστών και την υποστήριξή τους κατά την εγκατάσταση και τη χρήση του εργαλείου. Το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα.

58. Ιδίως στην περίπτωση των φυσικών προσώπων που δημοσιεύουν ελεύθερο λογισμικό ανοικτού κώδικα, η παροχή τεχνικής βοήθειας που συνδέεται άμεσα με την πρόσβαση στο προϊόν με ψηφιακά στοιχεία εξακολουθεί να μη θεωρείται εμπορική δραστηριότητα εάν, όπως αναφέρεται στην αιτιολογική σκέψη 15 του κανονισμού για την κυβερνοανθεκτικότητα, η χρέωση τιμήματος εξυπηρετεί μόνο την ανάκτηση του πραγματικού κόστους. Στις εν λόγω πραγματικές δαπάνες περιλαμβάνονται διάφορες δαπάνες που σχετίζονται με τον σχεδιασμό, την ανάπτυξη και τη συντήρηση του εν λόγω λογισμικού, συμπεριλαμβανομένων των εύλογων δαπανών διαβίωσης του προσώπου. Ως εκ τούτου, φυσικό πρόσωπο το οποίο δημοσιεύει ελεύθερο λογισμικό ανοικτού κώδικα και παρέχει τεχνική βοήθεια για την κάλυψη των δαπανών του και την εξασφάλιση εύλογης αμοιβής δεν πρέπει να θεωρείται, για τον λόγο αυτόν και μόνο, ότι θέτει το εν λόγω λογισμικό σε κυκλοφορία στην αγορά της ΕΕ.

59. Φυσικό ή νομικό πρόσωπο που παρέχει τεχνική βοήθεια σε σχέση με ελεύθερο λογισμικό ανοικτού κώδικα το οποίο δεν υπάγεται στην ευθύνη του δεν θεωρείται ότι θέτει το εν λόγω λογισμικό σε κυκλοφορία στην αγορά, εκτός εάν το εν λόγω πρόσωπο τροποποιήσει ουσιωδώς το ελεύθερο λογισμικό ανοικτού κώδικα, σύμφωνα με το άρθρο 22, στο πλαίσιο της παροχής της εν λόγω βοήθειας.

Παράδειγμα 19: Πάροχος υπηρεσιών δεν δημοσιεύει ελεύθερο λογισμικό ανοικτού κώδικα, αλλά βοηθά τον πελάτη να το εγκαταστήσει στον διακομιστή του εντός των εγκαταστάσεών του. Αυτό δε χωρίς ουσιαστική τροποποίηση του εν λόγω ελεύθερου λογισμικού ανοικτού κώδικα. Ως εκ τούτου, ο πάροχος υπηρεσιών δεν θεωρείται ότι θέτει το ελεύθερο λογισμικό ανοικτού κώδικα σε κυκλοφορία στην αγορά.

3.2.4. *Δωρεές*

60. Τα φυσικά ή νομικά πρόσωπα που δημοσιεύουν έργα ελεύθερου λογισμικού ανοικτού κώδικα περιλαμβάνουν συνήθως τρόπους με τους οποίους οι χρήστες του εν λόγω λογισμικού μπορούν να δωρίζουν οικειοθελώς χρήματα για να εκφράσουν τις ευχαριστίες τους προς τον εκδότη ή τους εκδότες του έργου και επίσης για να διασφαλίσουν την ενεργό συντήρηση του έργου.

61. Όπως αναφέρεται στην αιτιολογική σκέψη 15 του κανονισμού για την κυβερνοανθεκτικότητα «Η αποδοχή δωρεών χωρίς πρόθεση αποκόμισης κέρδους δεν θα πρέπει να θεωρείται εμπορική δραστηριότητα». Το γεγονός και μόνο της συμπερίληψης συνδέσμου προς πλατφόρμα δωρεών ή παρόμοια εργαλεία για τη συγκέντρωση δωρεών δεν θα πρέπει να θεωρείται πρόθεση αποκόμισης κέρδους, ακόμα και όταν το ποσό που εισπράττεται μέσω δωρεών υπερβαίνει το απλό κόστος που συνδέεται με τον σχεδιασμό, την ανάπτυξη και την παροχή ενός προϊόντος με ψηφιακά στοιχεία. Στο εν λόγω κόστος περιλαμβάνεται εύλογη αποζημίωση για τους συνεισφέροντες που προσλαμβάνονται από νομικό πρόσωπο και/ή εύλογες δαπάνες διαβίωσης φυσικού προσώπου. Οι δωρεές, από τη φύση τους, παρουσιάζουν διακυμάνσεις σε βάθος χρόνου και, ως εκ τούτου, πρέπει να υπάρχει ένας βαθμός ευελιξίας κατά την αξιολόγηση του αν ένα ελεύθερο λογισμικό ανοικτού κώδικα που αποφέρει οικονομικό όφελος αποκλειστικά μέσω δωρεών θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά. Ως εκ τούτου, ένα ελεύθερο λογισμικό ανοικτού κώδικα που υποστηρίζεται μόνο μέσω δωρεών δεν είναι πιθανό να θεωρηθεί ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα.

Παράδειγμα 20: Φυσικό ή νομικό πρόσωπο δημοσιεύει εργαλείο ελεύθερου λογισμικού ανοικτού κώδικα σε δημόσιο επιγραμμικό αποθετήριο, επιτρέποντας σε οποιονδήποτε να το καταφορτώνει, να το χρησιμοποιεί, να το τροποποιεί και να το αναδιανέμει βάσει άδειας ελεύθερης και ανοικτής πηγής. Ο εκδότης καλεί τους χρήστες να προβούν σε εθελοντικές δωρεές μέσω πλατφόρμας δωρεών για την υποστήριξη της συνεχούς ανάπτυξης και συντήρησης του έργου. Η πρόσβαση στο λογισμικό, στον πηγαίο κώδικα και στις ενημερώσεις του δεν εξαρτάται από την πραγματοποίηση δωρεάς. Το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα δεν θεωρείται ότι παρέχεται στο πλαίσιο εμπορικής δραστηριότητας και δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα.

62. Ωστόσο, υπάρχουν περιπτώσεις στις οποίες ένα ελεύθερο λογισμικό ανοικτού κώδικα που υποστηρίζεται μέσω δωρεών μπορεί να θεωρηθεί ότι τίθεται σε κυκλοφορία στην αγορά. Αυτό συμβαίνει όταν, βάσει συνολικής αξιολόγησης των περιστάσεων, οι δωρεές ισοδυναμούν εκ των πραγμάτων με χρέωση τιμήματος για την πρόσβαση στο προϊόν με ψηφιακά στοιχεία ή σε ορισμένες από τις λειτουργίες του. Ειδικότερα, αυτό μπορεί να συμβαίνει όταν η πρόσβαση στο ελεύθερο λογισμικό ανοικτού κώδικα, σε βασικές λειτουργίες ή σε ενημερώσεις εξαρτάται στην πράξη από την πραγματοποίηση δωρεάς ή όταν οι δωρεές συνδέονται με συμβατικά οφέλη ή αποκλειστικά πλεονεκτήματα που υπερβαίνουν τα προνόμια της κοινότητας.

Παράδειγμα 21: Φυσικό ή νομικό πρόσωπο δημοσιεύει προϊόν λογισμικού με ψηφιακά στοιχεία βάσει άδειας ελεύθερης και ανοικτής πηγής, αλλά παρέχει εκδόσεις και ενημερώσεις ασφαλείας που μπορούν να καταφορτωθούν μόνο από χρήστες που πραγματοποιούν δωρεά. Οι χρήστες που δεν πραγματοποιούν δωρεά δεν έχουν πρόσβαση στην τρέχουσα έκδοση του λογισμικού.

Στην περίπτωση αυτήν, οι δωρεές αποτελούν εκ των πραγμάτων προϋπόθεση για την πρόσβαση στο προϊόν με ψηφιακά στοιχεία και, ως εκ τούτου, ισοδυναμούν με χρέωση τιμήματος. Ως εκ τούτου, το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα.

Παράδειγμα 22: Φυσικό ή νομικό πρόσωπο δημοσιοποιεί τον πηγαίο κώδικα ενός ελεύθερου λογισμικού ανοικτού κώδικα, αλλά παρέχει προ-μεταγλωττισμένα δυαδικά αρχεία, τακτικές ενημερώσεις και εγγυημένες διορθώσεις ασφαλείας μόνο στους δωρητές. Στην περίπτωση αυτήν, οι δωρεές συνδέονται με την πρόσβαση σε βασικές πτυχές του προϊόντος με ψηφιακά στοιχεία και αποτελούν αμοιβή για την προμήθεια του εν λόγω προϊόντος. Επομένως, το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά στο πλαίσιο εμπορικής δραστηριότητας.

3.2.5. *Χρηματοδότηση ελεύθερου λογισμικού ανοικτού κώδικα*

63. Το γεγονός και μόνο ότι τρίτος πλήρωσε, προέβη σε χορηγία ή χρηματοδότησε με άλλον τρόπο την ανάπτυξη ελεύθερου λογισμικού ανοικτού κώδικα δεν καθορίζει, από μόνο του, αν το ελεύθερο λογισμικό ανοικτού κώδικα τίθεται σε κυκλοφορία στην αγορά. Αποτελεί συνήθη πρακτική στο οικοσύστημα ελεύθερου λογισμικού ανοικτού κώδικα οι μεμονωμένοι προγραμματιστές, ιδρύματα ή κοινότητες να λαμβάνουν χρηματοδότηση από εταιρείες, δημόσιους φορείς ή άλλους χορηγούς προκειμένου να εργαστούν σε συγκεκριμένα χαρακτηριστικά, να διορθώσουν σφάλματα ή να συντηρήσουν δομοστοιχεία κρίσιμης σημασίας. Η χρηματοδότηση αυτή μπορεί να λάβει πολλές μορφές, συμπεριλαμβανομένων των επιχορηγήσεων, των προγραμμάτων ανεύρεσης ευπαθειών («bug bounties»), των χορηγιών, των συμβάσεων παροχής υπηρεσιών ή των αμειβομένων εργασιών ανάπτυξης.

64. Όπως υπενθυμίστηκε ήδη, στην αιτιολογική σκέψη 18 του κανονισμού για την κυβερνοανθεκτικότητα διευκρινίζεται ότι κατά τον προσδιορισμό του εμπορικού χαρακτήρα της εν λόγω δραστηριότητας, δεν θα πρέπει να λαμβάνονται υπόψη από μόνες τους οι συνθήκες υπό τις οποίες αναπτύχθηκε το προϊόν με ψηφιακά στοιχεία ή ο τρόπος με τον οποίο έχει χρηματοδοτηθεί η ανάπτυξη.

65. Ως εκ τούτου, όταν το ελεύθερο λογισμικό ανοικτού κώδικα διανέμεται ανοικτά και διατίθεται ελεύθερα σε όλους για πρόσβαση, χρήση, τροποποίηση και αναδιανομή, το γεγονός ότι μια εμπορική οντότητα ενδέχεται να έχει πληρώσει για το εν λόγω έργο δεν θα πρέπει να λαμβάνεται υπόψη κατά τον προσδιορισμό του αν το λογισμικό τίθεται σε κυκλοφορία στην αγορά. Στην πραγματικότητα, εάν το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα δεν αποφέρει οικονομικό όφελος με άλλον τρόπο, δεν πρέπει να θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά. Όταν η εταιρεία που χρηματοδότησε την ανάπτυξη του ελεύθερου λογισμικού ανοικτού κώδικα (καθώς και οποιαδήποτε άλλη εταιρεία) το ενσωματώνει στο προϊόν της με ψηφιακά στοιχεία, η εν λόγω εταιρεία πρέπει να επιδεικνύει τη δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5 του κανονισμού για την κυβερνοανθεκτικότητα.

Παράδειγμα 23: Μεμονωμένος προγραμματιστής δημοσιεύει έργο ελεύθερου λογισμικού ανοικτού κώδικα και το συντηρεί ενεργά. Ο κατασκευαστής Α ζητεί από τον μεμονωμένο προγραμματιστή να προσθέσει ένα ειδικό χαρακτηριστικό για το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα και να χρηματοδοτήσει την εν λόγω ανάπτυξη. Ο προγραμματιστής προσθέτει το χαρακτηριστικό στη βάση κώδικα του ελεύθερου λογισμικού ανοικτού κώδικα, διανέμοντάς την ανοικτά και καθιστώντας την ελεύθερα διαθέσιμη σε όλους για πρόσβαση, χρήση, τροποποίηση και αναδιανομή. Ο μεμονωμένος προγραμματιστής δεν θεωρείται ότι έχει θέσει το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα σε κυκλοφορία στην αγορά. Εάν ο κατασκευαστής ενσωματώνει το ελεύθερο λογισμικό ανοικτού κώδικα στο προϊόν του με ψηφιακά στοιχεία, πρέπει να επιδεικνύει τη δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5.

3.2.6. *Μη κερδοσκοπικές οντότητες που έχουν συσταθεί για την επίτευξη μη κερδοσκοπικών στόχων*

66. Όταν ένα νομικό πρόσωπο που δημοσιεύει ελεύθερο λογισμικό ανοικτού κώδικα είναι μη κερδοσκοπικός οργανισμός που «έχει συσταθεί κατά τρόπο που διασφαλίζει ότι όλα τα έσοδα μετά την κάλυψη του κόστους χρησιμοποιούνται για την επίτευξη μη κερδοσκοπικών στόχων» (αιτιολογική σκέψη 18 του κανονισμού για την κυβερνοανθεκτικότητα), το ελεύθερο λογισμικό ανοικτού κώδικα που δημοσιεύει δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά. Όταν το εν λόγω νομικό πρόσωπο πληροί τον ορισμό του «υποστηρικτή», υπόκειται στις αντίστοιχες υποχρεώσεις (άρθρο 24 του κανονισμού για την κυβερνοανθεκτικότητα).

Παράδειγμα 24: Νομικό πρόσωπο δημοσιεύει ελεύθερο πρόγραμμα περιήγησης ανοικτού κώδικα που προσκομίζει άμεσο οικονομικό όφελος μέσω συμπράξεων με μηχανές αναζήτησης, αλλά όλα τα έσοδά του μετά την κάλυψη του κόστους χρησιμοποιούνται για μη κερδοσκοπικούς στόχους. Το πρόγραμμα περιήγησης δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα. Το νομικό πρόσωπο που το δημοσιεύει υπόκειται στις υποχρεώσεις που ισχύουν για τους υποστηρικτές.

3.2.7. *Ενσωμάτωση από άλλους κατασκευαστές*

67. Σε ορισμένες περιπτώσεις, το ελεύθερο λογισμικό ανοικτού κώδικα δημοσιεύεται από σαφώς αναγνωρίσιμο φυσικό ή νομικό πρόσωπο, αλλά το ελεύθερο λογισμικό ανοικτού κώδικα «προορίζεται για ενσωμάτωση από άλλους κατασκευαστές στα δικά τους προϊόντα με ψηφιακά στοιχεία». Στις περιπτώσεις αυτές, το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά της ΕΕ, εκτός εάν αποκομίζει οικονομικό όφελος και το πρόσωπο που το δημοσιεύει (δηλαδή ο αρχικός κατασκευαστής), σύμφωνα με τα προηγούμενα τμήματα της παρούσας καθοδήγησης.

68. Όταν το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα δεν τίθεται σε κυκλοφορία στην αγορά, το νομικό πρόσωπο που το δημοσιεύει θα υπόκειται στις υποχρεώσεις των υποστηρικτών, εάν παρέχει υποστήριξη σε διαρκή βάση, σύμφωνα με τον ορισμό του «υποστηρικτή».

Παράδειγμα 25: Νομικό πρόσωπο δημοσιεύει βιβλιοθήκη ελεύθερου λογισμικού ανοικτού κώδικα για τη δημιουργία διεπαφών χρήστη. Δεν αποκομίζει οικονομικό όφελος για την προμήθεια της εν λόγω βιβλιοθήκης, αλλά την ενσωματώνει σε ένα από τα προϊόντα του με ψηφιακά στοιχεία (το οποίο με τη σειρά του τίθεται σε κυκλοφορία στην αγορά). Η βιβλιοθήκη δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα, αλλά προορίζεται για ενσωμάτωση σε προϊόντα με ψηφιακά στοιχεία. Το νομικό πρόσωπο που τη δημοσιεύει είναι ο υποστηρικτής της.

Παράδειγμα 26: Νομικό πρόσωπο θέτει λειτουργικό σύστημα σε κυκλοφορία στην αγορά και δημοσιεύει επίσης βιβλιοθήκες ελεύθερου λογισμικού ανοικτού κώδικα που χρησιμεύουν ως εφαρμογές αναφοράς για τους χρήστες του εν λόγω λειτουργικού συστήματος. Το νομικό πρόσωπο δεν αποκομίζει οικονομικό όφελος από τις βιβλιοθήκες ελεύθερου λογισμικού ανοικτού κώδικα, οι οποίες προορίζονται για ενσωμάτωση σε άλλα προϊόντα με ψηφιακά στοιχεία. Το νομικό πρόσωπο που τις δημοσιεύει είναι υποστηρικτής των εν λόγω βιβλιοθηκών ελεύθερου λογισμικού ανοικτού κώδικα.

3.3. **Υποστηρικτές λογισμικού ανοικτού κώδικα**

69. Ο κανονισμός για την κυβερνοανθεκτικότητα εισάγει τη νέα νομική κατηγορία του «υποστηρικτή λογισμικού ανοικτού κώδικα» λαμβάνοντας υπόψη «τη σημασία που έχουν για την κυβερνοασφάλεια πολλά προϊόντα με ψηφιακά στοιχεία κατατασσόμενα στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία δημοσιεύονται αλλά δεν διατίθενται στην αγορά κατά την έννοια του [κανονισμού για την κυβερνοανθεκτικότητα]» (αιτιολογική σκέψη 19 του κανονισμού για την κυβερνοανθεκτικότητα).

70. Σε ορισμένες περιπτώσεις, ένα ελεύθερο λογισμικό ανοικτού κώδικα δημοσιεύεται αλλά δεν διατίθεται στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα από νομικό πρόσωπο το οποίο «έχει σκοπό ή στόχο να παρέχει συστηματικά υποστήριξη σε διαρκή βάση για την ανάπτυξη [ελεύθερου λογισμικού ανοικτού κώδικα] [...] [που] προορίζ[ε]ται για εμπορικές δραστηριότητες, και το οποίο διασφαλίζει τη βιωσιμότητα των εν λόγω προϊόντων» [άρθρο 3 σημείο 14) του κανονισμού για την κυβερνοανθεκτικότητα]. Στις περιπτώσεις αυτές, το εν λόγω νομικό πρόσωπο υπόκειται στις υποχρεώσεις των υποστηρικτών.

71. Ως υποστηρικτής ορίζεται «νομικό πρόσωπο, άλλο από τον κατασκευαστή», διότι κατασκευαστής είναι εξ ορισμού το φυσικό ή νομικό πρόσωπο που θέτει προϊόντα με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά («τα διαθέτει στην αγορά») υπό την επωνυμία ή το εμπορικό σήμα του. Ένα νομικό πρόσωπο μπορεί να είναι υποστηρικτής μόνο προϊόντων με ψηφιακά στοιχεία που χαρακτηρίζονται ως ελεύθερο λογισμικό ανοικτού κώδικα και τα οποία δημοσιεύονται αλλά δεν διατίθενται στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα. Ως εκ τούτου, η έννοια του υποστηρικτή εφαρμόζεται σε συγκεκριμένες περιπτώσεις ελεύθερου λογισμικού ανοικτού κώδικα όπου «ο τελικός προορισμός είναι εμπορικές δραστηριότητες, όπως ενσωμάτωση σε εμπορικές υπηρεσίες ή σε προϊόντα με ψηφιακά στοιχεία παρεχόμενα έναντι οικονομικού οφέλους» (αιτιολογική σκέψη 19 του κανονισμού για την κυβερνοανθεκτικότητα ([13])), αλλά στις οποίες δεν πραγματοποιείται διάθεση στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα και στις οποίες το νομικό πρόσωπο που δημοσιεύει το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα διασφαλίζει τη συστηματική του υποστήριξη.

72. Η ιδιότητα του υποστηρικτή για ένα συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα δεν συνεπάγεται ότι το εν λόγω νομικό πρόσωπο είναι κατ' ανάγκη και υποστηρικτής για άλλα ελεύθερα λογισμικά ανοικτού κώδικα τα οποία δημοσιεύει. Ομοίως, η ιδιότητα του κατασκευαστή για ένα συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα δεν συνεπάγεται ότι το νομικό πρόσωπο δεν μπορεί να είναι υποστηρικτής για άλλα ελεύθερα λογισμικά ανοικτού κώδικα. Στο πλαίσιο αυτό περιλαμβάνεται η παροχή εκδόσεων «κοινότητας» του ίδιου ελεύθερου λογισμικού ανοικτού κώδικα, όπως περιγράφεται στο τμήμα *3.2.1 Charging a price*.

73. Ως εκ τούτου, ένα νομικό πρόσωπο μπορεί να είναι ταυτόχρονα υποστηρικτής για ένα συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα (όταν ο υποστηρικτής παρέχει συστηματικά υποστήριξη σε διαρκή βάση και διασφαλίζει τη βιωσιμότητα του λογισμικού) και κατασκευαστής για άλλο συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα (όταν το θέτει σε κυκλοφορία στην αγορά). Με άλλα λόγια, η ίδια νομική οντότητα μπορεί να κληθεί να εκπληρώσει διαφορετικούς ρόλους για διαφορετικά έργα ελεύθερου λογισμικού ανοικτού κώδικα.

74. Για κάθε συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα που δημοσιεύει, το νομικό πρόσωπο θα πρέπει να διακριβώνει αν το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα. Στην περίπτωση αυτήν, η νομική οντότητα καθίσταται ο κατασκευαστής του λογισμικού. Εάν το ελεύθερο λογισμικό ανοικτού κώδικα δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά, το νομικό πρόσωπο μπορεί να είναι ο υποστηρικτής του, εάν το λογισμικό προορίζεται για εμπορικές δραστηριότητες και εάν το νομικό πρόσωπο το υποστηρίζει σύμφωνα με τον ορισμό του υποστηρικτή ([14]).

3.3.1. *Διαρκής υποστήριξη και διασφάλιση της βιωσιμότητας του ελεύθερου λογισμικού ανοικτού κώδικα*

75. Στην αιτιολογική σκέψη 19 διευκρινίζεται ότι η παροχή διαρκούς υποστήριξης για την ανάπτυξη ενός προϊόντος με ψηφιακά στοιχεία μπορεί να περιλαμβάνει (μεταξύ άλλων): i) τη φιλοξενία και τη διαχείριση πλατφορμών συνεργασίας για την ανάπτυξη λογισμικού· ii) τη φιλοξενία πηγαίου κώδικα ή λογισμικού· iii) τη διακυβέρνηση ή τη διαχείριση προϊόντων με ψηφιακά στοιχεία κατατασσόμενων στο ελεύθερο λογισμικό ανοικτού κώδικα· και iv) την καθοδήγηση της ανάπτυξης των εν λόγω προϊόντων με ψηφιακά στοιχεία.

76. Αυτό μπορεί να ισχύει, για παράδειγμα, για νομική οντότητα που αναπτύσσει ελεύθερο λογισμικό ανοικτού κώδικα για ενσωμάτωση στα δικά της προϊόντα με ψηφιακά στοιχεία και στη συνέχεια το δημοσιεύει χωρίς να το θέτει σε κυκλοφορία στην αγορά. Το ζήτημα αυτό εξετάζεται επίσης στο τμήμα *3.2.7 Integration by other manufacturers*. Στην περίπτωση αυτήν, η νομική οντότητα δεν είναι κατασκευαστής του λογισμικού, αλλά μπορεί να είναι υποστηρικτής του. Επιπλέον, όπως εξηγείται στα προηγούμενα τμήματα, νομική οντότητα που δημοσιεύει ελεύθερη έκδοση (ή έκδοση κοινότητας) και έκδοση του ίδιου ελεύθερου λογισμικού ανοικτού κώδικα έναντι οικονομικού οφέλους θεωρείται υποστηρικτής της ελεύθερης έκδοσης (ή της έκδοσης κοινότητας) και κατασκευαστής της έκδοσης έναντι οικονομικού οφέλους.

77. Ομοίως, νομική οντότητα που αποκομίζει οικονομικό όφελος από ελεύθερο λογισμικό ανοικτού κώδικα, αλλά είναι μη κερδοσκοπική οντότητα της οποίας τα έσοδα μετά την κάλυψη του κόστους χρησιμοποιούνται για την επίτευξη μη κερδοσκοπικών στόχων (και, ως εκ τούτου, το οικείο ελεύθερο λογισμικό ανοικτού κώδικα δεν τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα, όπως αναλύεται στο τμήμα *3.2.6 Not-for-profit entities*) αποτελεί υποστηρικτή του ελεύθερου λογισμικού ανοικτού κώδικα που δημοσιεύει.

78. Επιπλέον, ορισμένα ιδρύματα προσφέρουν πλατφόρμες συνεργασίας με διάφορες μορφές διακυβέρνησης που επιτρέπουν στους κατασκευαστές να συμβάλλουν τακτικά στην ανάπτυξη ελεύθερου λογισμικού ανοικτού κώδικα και/ή που χρηματοδοτούνται τακτικά από τους κατασκευαστές. Τα ιδρύματα αυτά πρέπει να θεωρούνται υποστηρικτές σε σχέση με συγκεκριμένα ελεύθερα λογισμικά ανοικτού κώδικα που προορίζονται για εμπορικές δραστηριότητες και για τα οποία το ίδρυμα παρέχει διαρκή υποστήριξη. Ωστόσο, όπως εξηγείται στο τμήμα *3.3 Open-source software stewards*, ένα τέτοιο ίδρυμα μπορεί να μην υπόκειται σε υποχρεώσεις στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα για άλλα συγκεκριμένα ελεύθερα λογισμικά ανοικτού κώδικα που φιλοξενεί, σε περιπτώσεις όπου δεν παρέχει συστηματική υποστήριξη για συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα, δεν διασφαλίζει τη βιωσιμότητά του και/ή το συγκεκριμένο λογισμικό δεν προορίζεται για εμπορικές δραστηριότητες.

([13]) Η έννοια αυτή περιλαμβάνεται επίσης στη διατύπωση «που προορίζονται για εμπορικές δραστηριότητες» η οποία περιλαμβάνεται στον ορισμό του «υποστηρικτή λογισμικού ανοικτού κώδικα» που παρατίθεται στο άρθρο 3 σημείο 14) του κανονισμού για την κυβερνοανθεκτικότητα.

([14]) Το νομικό πρόσωπο μπορεί επίσης να μην υπόκειται σε υποχρεώσεις που απορρέουν από τον κανονισμό για την κυβερνοανθεκτικότητα, σε περιπτώσεις κατά τις οποίες: i) ένα συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα δεν τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα· και ii) η νομική οντότητα δεν πληροί τον ορισμό του υποστηρικτή σε σχέση με το συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα.

79. Το είδος της «διαρκούς υποστήριξης» που παρέχουν ιδρύματα και παρόμοιοι οργανισμοί σε συγκεκριμένα έργα ελεύθερου λογισμικού ανοικτού κώδικα μπορεί να ποικίλλει σημαντικά. Για παράδειγμα, ορισμένες νομικές οντότητες παρέχουν μόνο μη τεχνική υποστήριξη, όπως η διαχείριση της δημιουργίας εμπορικού σήματος των έργων, η θέσπιση κανόνων διακυβέρνησης, η διοργάνωση κοινοτικών εκδηλώσεων ή η συγκέντρωση δωρεών. Άλλες οντότητες παρέχουν επίσης την υποκείμενη υποδομή ΤΠ που είναι αναγκαία για την εκτέλεση του έργου, όπως φιλοξενία αποθετηρίων πηγαίου κώδικα, παροχή συστημάτων ελέγχου εκδόσεων ή δημιουργία κλειδιών υπογραφής. Άλλες προχωρούν περαιτέρω στο είδος της υποστήριξης που παρέχουν συνεισφέροντας ενεργά τεχνικούς πόρους στο έργο, για παράδειγμα με την απασχόληση προγραμματιστών, τον συντονισμό των εργασιών ανάπτυξης, την επανεξέταση ή τη συγχώνευση κώδικα, τη διαχείριση εκδόσεων ή τον χειρισμό εκθέσεων ευπαθειών και διορθώσεων ασφαλείας. Ενώ όλες οι νομικές οντότητες που χαρακτηρίζονται ως υποστηρικτές στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα υποχρεούνται να συμμορφώνονται με τις υποχρεώσεις του άρθρου 24 παράγραφοι 1 και 2, ο βαθμός στον οποίο οι υποχρεώσεις που ορίζονται στο άρθρο 14 παράγραφοι 1, 3 και 8 ισχύουν για τις εν λόγω νομικές οντότητες διαφέρει ανάλογα με το είδος της υποστήριξης που παρέχουν, σύμφωνα με το άρθρο 24 παράγραφος 3.

80. Για παράδειγμα, ένας υποστηρικτής που παρέχει μόνο μη τεχνική υποστήριξη δεν συμμετέχει, εξ ορισμού, στην ανάπτυξη του προϊόντος με ψηφιακά στοιχεία και, ως εκ τούτου, δεν υποχρεούται να αναφέρει ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης. Ο εν λόγω υποστηρικτής δεν παρέχει επίσης συστήματα δικτύου και πληροφοριών για την ανάπτυξη τέτοιων προϊόντων με ψηφιακά στοιχεία και, ως εκ τούτου, δεν υποχρεούται να αναφέρει σοβαρά περιστατικά στον ENISA και στις ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (ΟΑΠΑΥ) ή στους επηρεαζόμενους χρήστες. Ωστόσο, όταν ο υποστηρικτής αντιληφθεί μια ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης (π.χ. μέσω έκθεσης από εξωτερικές πηγές, όπως ερευνητές στον τομέα της ασφάλειας), θα πρέπει να κοινοποιεί τις πληροφορίες στους συντηρητές του προϊόντος με ψηφιακά στοιχεία, σύμφωνα με την πολιτική του για την κυβερνοασφάλεια. Οι συντηρητές των προϊόντων με ψηφιακά στοιχεία και/ή οι υποστηρικτές θα πρέπει επίσης να εξετάζουν το ενδεχόμενο αναφοράς της ευπάθειας σε εθελοντική βάση, σύμφωνα με το άρθρο 15.

81. Από την άλλη πλευρά, όταν ένας υποστηρικτής παρέχει την υποκείμενη υποδομή ΤΠ για ορισμένα προϊόντα με ψηφιακά στοιχεία, υποχρεούται να κοινοποιεί στον ENISA και στις ΟΑΠΑΥ, σύμφωνα με το άρθρο 14 παράγραφος 3, τυχόν σοβαρά περιστατικά που σχετίζονται με την εν λόγω υποδομή και έχουν αντίκτυπο στην ασφάλεια των προϊόντων με ψηφιακά στοιχεία. Απαιτείται επίσης, κατά περίπτωση, να ενημερώνει όλους τους χρήστες (π.χ. μέσω γενικής ανακοίνωσης). Όπως αναφέρεται στο προηγούμενο σημείο, μολονότι ο υποστηρικτής δεν υποχρεούται να αναφέρει τις ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και οι οποίες υποπίπτουν στην αντίληψή του, θα πρέπει να προωθεί τον ορθό χειρισμό των ευπαθειών και να εξετάζει το ενδεχόμενο εθελοντικής αναφοράς σύμφωνα με το άρθρο 15.

82. Τέλος, όταν ένας υποστηρικτής παρέχει επίσης τεχνικούς πόρους σε συγκεκριμένα προϊόντα με ψηφιακά στοιχεία, υποχρεούται: i) να κοινοποιεί, σύμφωνα με το άρθρο 14 παράγραφος 1, τις ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και οι οποίες υποπίπτουν στην αντίληψή του· και ii) κατά περίπτωση, να ενημερώνει όλους τους χρήστες. Στον βαθμό που ο υποστηρικτής έχει επίσης άμεση σχέση με τους επηρεαζόμενους χρήστες, υποχρεούται επίσης να τους ενημερώνει απευθείας, σύμφωνα με το άρθρο 14 παράγραφος 8.

83. Όταν μια οντότητα παύει να παρέχει συστηματική στήριξη σε διαρκή βάση για ένα συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα, ενδέχεται να μην πληροί πλέον τον ορισμό του υποστηρικτή και, ως εκ τούτου, να μην υπόκειται πλέον στις αντίστοιχες υποχρεώσεις. Στις περιπτώσεις αυτές, η εν λόγω οντότητα ενθαρρύνεται να κοινοποιεί με σαφήνεια τη μεταβολή του καθεστώτος της για το συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα.

84. Σε ορισμένες περιπτώσεις, μια οντότητα που ήταν υποστηρικτής συγκεκριμένου έργου μπορεί να αποφασίσει να αποκομίσει οικονομικό όφελος από το εν λόγω έργο απευθείας, θέτοντας έτσι το προϊόν με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά και ενεργοποιώντας τις υποχρεώσεις του κατασκευαστή στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα. Υπό τις συνθήκες αυτές, η εν λόγω οντότητα μπορεί να χαρακτηριστεί ως ο κατασκευαστής του προϊόντος με ψηφιακά στοιχεία από την ημερομηνία κατά την οποία το θέτει σε κυκλοφορία στην αγορά (αλλά όχι όσον αφορά προγενέστερες εκδόσεις για τις οποίες ενήργησε ως υποστηρικτής).

3.4. **Συνεισφέροντες και κατάντη χρήσεις**

85. Όπως αναφέρθηκε ήδη στο τμήμα *3.1 Determining if free and open-source software is* under one's responsibility, στον κανονισμό για την κυβερνοανθεκτικότητα διευκρινίζεται ότι ο κανονισμός «δεν εφαρμόζεται σε φυσικά ή νομικά πρόσωπα που συνεισφέρουν με πηγαίο κώδικα σε προϊόντα με ψηφιακά στοιχεία κατατασσόμενα στο ελεύθερο λογισμικό ανοικτού κώδικα τα οποία δεν τελούν υπό την ευθύνη τους» (αιτιολογική σκέψη 18).

86. Οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία που ενσωματώνουν δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία επίσης δεν καθίστανται υπεύθυνοι για την ατομική συμμόρφωση των εν λόγω δομοστοιχείων με τον κανονισμό για την κυβερνοανθεκτικότητα, ακόμα και όταν οι κατασκευαστές συνεισφέρουν τον πηγαίο κώδικα για τη συντήρησή τους.

87. Ομοίως, το γεγονός και μόνο ότι οι κατασκευαστές ενσωματώνουν δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία (από τα οποία αποκομίζουν οικονομικό όφελος) δεν επηρεάζει τον χαρακτήρα του εν λόγω δομοστοιχείου ελεύθερου λογισμικού ανοικτού κώδικα στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα. Οι συντηρητές δομοστοιχείων ελεύθερου λογισμικού ανοικτού κώδικα που δεν τίθενται σε κυκλοφορία στην αγορά δεν υπέχουν υποχρεώσεις σχετικά με άλλες οντότητες που μπορούν να ενσωματώσουν τα εν λόγω δομοστοιχεία στα προϊόντα τους με ψηφιακά στοιχεία. Το αν ο κανονισμός για την κυβερνοανθεκτικότητα εφαρμόζεται σε ένα δεδομένο δομοστοιχείο ελεύθερου λογισμικού ανοικτού κώδικα εξαρτάται αποκλειστικά από το αν το φυσικό ή νομικό πρόσωπο που το δημοσιεύει το θέτει σε κυκλοφορία στην αγορά.

88. Ωστόσο, οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία που ενσωματώνουν δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα υποχρεούνται να συμμορφώνονται με τον κανονισμό για την κυβερνοανθεκτικότητα για τα δικά τους προϊόντα με ψηφιακά στοιχεία. Υπέχουν επίσης υποχρέωση δέουσας επιμέλειας, σύμφωνα με το άρθρο 13 παράγραφος 5, όσον αφορά τα δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα που ενσωματώνουν. Επιπλέον, υποχρεούνται να αναφέρουν τις ευπάθειες των ενσωματωμένων δομοστοιχείων και να διανέμουν τις διορθώσεις ασφαλείας σύμφωνα με το άρθρο 13 παράγραφος 6. Για περισσότερη καθοδήγηση σχετικά με το θέμα αυτό, βλ. τμήμα *9.2.1 Reporting upstream and sharing security fixes*.

3.5. **Ενδεικτικά σενάρια**

89. Τα παραδείγματα που παρατίθενται κατωτέρω είναι εντελώς υποθετικά και αποσκοπούν μόνο στην παρουσίαση διαφορετικών περιπτώσεων, όπως εξηγούνται στα ανωτέρω τμήματα.

Παράδειγμα 27: Μεμονωμένος προγραμματιστής Α έχει αναπτύξει ελεύθερο λογισμικό ανοικτού κώδικα. Ο προγραμματιστής Α δημοσιεύει το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα υπό τη δική του επωνυμία ή εμπορικό σήμα, χωρίς να χρεώνει για τη χρήση του. Το λογισμικό διανέμεται ανοικτά και διατίθεται ελεύθερα σε όλους για πρόσβαση, χρήση, τροποποίηση και αναδιανομή. Ο προγραμματιστής Α περιλαμβάνει επίσης σύνδεσμο προς πλατφόρμα για τη συγκέντρωση εθελοντικών δωρεών.

Οι εταιρείες Β, Γ και Δ ενσωματώνουν το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία. Για την υποστήριξη της συνεχούς συντήρησης, οι εταιρείες Β, Γ και Δ πραγματοποιούν εθελοντικές δωρεές στον προγραμματιστή Α. Οι δωρεές αυτές επιτρέπουν στον προγραμματιστή Α να συντηρεί ενεργά το έργο.

Το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα δεν τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα. Ο προγραμματιστής Α δεν υπέχει υποχρεώσεις στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα. Οι εταιρείες Β, Γ και Δ πρέπει να επιδεικνύουν δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5 κατά την ενσωμάτωση του εν λόγω ελεύθερου λογισμικού ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία.

Παράδειγμα 28: Το μη κερδοσκοπικό ίδρυμα ΣΤ δημοσιεύει δομοστοιχείο ελεύθερου λογισμικού ανοικτού κώδικα για ενσωμάτωση σε άλλα εμπορικά προϊόντα με ψηφιακά στοιχεία. Το ίδρυμα ΣΤ δεσμεύεται να παρέχει διαρκή υποστήριξη στο εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα, ώστε να διασφαλίζεται η βιωσιμότητα και η υιοθέτησή του. Οι εταιρείες Α, Β και Γ ενσωματώνουν το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία. Οι εταιρείες Α και Β συνεισφέρουν οικειοθελώς μέρος του χρόνου των προγραμματιστών τους για την ανάπτυξη και τη συντήρηση έργων ελεύθερου λογισμικού ανοικτού κώδικα εντός του ιδρύματος ΣΤ, μεταξύ άλλων και για το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα.

Δεδομένου ότι το ίδρυμα ΣΤ είναι μη κερδοσκοπική οντότητα που έχει συσταθεί με τρόπο ώστε τα έσοδά του μετά την κάλυψη του κόστους να χρησιμοποιούνται για την επίτευξη μη κερδοσκοπικών στόχων, το ελεύθερο λογισμικό ανοικτού κώδικα δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα. Το ίδρυμα ΣΤ είναι ο υποστηρικτής του ελεύθερου λογισμικού ανοικτού κώδικα και υπόκειται στις αντίστοιχες υποχρεώσεις που προβλέπονται στο άρθρο 24. Οι εταιρείες Α, Β και Γ πρέπει να επιδεικνύουν δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5 κατά την ενσωμάτωση του εν λόγω ελεύθερου λογισμικού ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία.

Παράδειγμα 29: Εταιρεία Α έχει αναπτύξει δομοστοιχείο ελεύθερου λογισμικού ανοικτού κώδικα για ενσωμάτωση στα δικά της προϊόντα με ψηφιακά στοιχεία. Δημοσιεύει επίσης το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα χωριστά υπό τη δική της επωνυμία ή εμπορικό σήμα και το συντηρεί ενεργά. Ωστόσο, δεν χρεώνει για τη χρήση του ούτε αποκομίζει οικονομικό όφελος με άλλους τρόπους. Οι εταιρείες Β, Γ και Δ ενσωματώνουν το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία και συνεισφέρουν οικειοθελώς μέρος του χρόνου των προγραμματιστών τους για τη συντήρησή του.

Το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα δεν θεωρείται ότι τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα. Η εταιρεία Α δεν είναι ο κατασκευαστής του, αλλά ο υποστηρικτής του. Οι εταιρείες Β, Γ και Δ πρέπει να επιδεικνύουν δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5 κατά την ενσωμάτωση του ελεύθερου λογισμικού ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία.

Παράδειγμα 30: Η εταιρεία Α δημοσιεύει ελεύθερο λογισμικό ανοικτού κώδικα υπό τη δική της επωνυμία ή εμπορικό σήμα και το προσφέρει ως έκδοση επί πληρωμή, η οποία περιλαμβάνει ορισμένα οφέλη, όπως τεχνική βοήθεια ή βελτιστοποίηση των επιδόσεων. Οι προγραμματιστές των εταιρειών Β, Γ και Δ συνεισφέρουν στη συντήρηση του ελεύθερου λογισμικού ανοικτού κώδικα, το οποίο, ωστόσο, παραμένει υπό τον έλεγχο της εταιρείας Α.

Η εταιρεία Α θεωρείται κατασκευαστής του εν λόγω ελεύθερου λογισμικού ανοικτού κώδικα ([15]). Οι εταιρείες Β, Γ και Δ δεν υπόκεινται στις υποχρεώσεις που απορρέουν από τον κανονισμό για την κυβερνοανθεκτικότητα για το συγκεκριμένο ελεύθερο λογισμικό ανοικτού κώδικα. Εάν ενσωματώνουν το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα στα δικά τους προϊόντα με ψηφιακά στοιχεία, υποχρεούνται να επιδεικνύουν δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5.

Παράδειγμα 31: Η εταιρεία Α δημοσιεύει ελεύθερο λογισμικό ανοικτού κώδικα υπό τη δική της επωνυμία ή εμπορικό σήμα και παρέχει διαρκή συντήρηση για να διασφαλίζεται η μακροπρόθεσμη βιωσιμότητά του, ώστε να είναι δυνατή η ενσωμάτωση του εν λόγω λογισμικού σε προϊόντα άλλων εταιρειών με ψηφιακά στοιχεία. Η εταιρεία Α δεν επιβάλλει χρέωση για τη χρήση του, δεν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα που συλλέγει μέσω του προϊόντος με ψηφιακά στοιχεία ούτε πωλεί υπηρεσίες υποστήριξης που συνδέονται με τη δημοσίευση του ελεύθερου λογισμικού ανοικτού κώδικα.

Η εταιρεία Β συνεισφέρει κώδικα και χρόνο προγραμματιστών για τη συντήρηση του ελεύθερου λογισμικού ανοικτού κώδικα, αλλά δεν το διανέμει εμπορικά. Η εταιρεία Β παρέχει υπηρεσίες τεχνικής υποστήριξης ανεξάρτητα από τη διανομή του ελεύθερου λογισμικού ανοικτού κώδικα. Η εταιρεία Α θεωρείται ότι είναι ο υποστηρικτής του εν λόγω ελεύθερου λογισμικού ανοικτού κώδικα, ενώ η εταιρεία Β δεν υπέχει υποχρεώσεις βάσει του κανονισμού για την κυβερνοανθεκτικότητα για το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα.

Παράδειγμα 32: Δομοστοιχείο ελεύθερου λογισμικού ανοικτού κώδικα δημοσιεύεται από μη κερδοσκοπική οντότητα που έχει συσταθεί με τρόπο που διασφαλίζει ότι όλα τα έσοδα μετά την κάλυψη του κόστους χρησιμοποιούνται για την επίτευξη μη κερδοσκοπικών στόχων. Η οντότητα παρέχει διαρκή υποστήριξη με σκοπό τη διασφάλιση της μακροπρόθεσμης βιωσιμότητας του έργου. Η συντήρηση χρηματοδοτείται μέσω δημόσιας χρηματοδότησης, όπως επιχορηγήσεις έρευνας. Επιπλέον αναπτύξεις, όπως νέων χαρακτηριστικών, χρηματοδοτούνται μέσω δωρεών και ειδικών έργων, τα οποία υλοποιούνται σε συνεργασία με κατασκευαστές που ενσωματώνουν το εν λόγω ελεύθερο λογισμικό ανοικτού κώδικα στα προϊόντα τους με ψηφιακά στοιχεία. Τα χαρακτηριστικά αυτά ενσωματώνονται στη βάση κώδικα του ελεύθερου λογισμικού ανοικτού κώδικα.

Η μη κερδοσκοπική οντότητα που δημοσιεύει το ελεύθερο λογισμικό ανοικτού κώδικα θεωρείται ο υποστηρικτής του εν λόγω δομοστοιχείου του ελεύθερου λογισμικού ανοικτού κώδικα. Κατασκευαστής που έχει συνεισφέρει στην ανάπτυξη ορισμένων χαρακτηριστικών δεν καθίσταται κατασκευαστής του εν λόγω δομοστοιχείου του ελεύθερου λογισμικού ανοικτού κώδικα. Όταν ο κατασκευαστής ενσωματώνει το εν λόγω δομοστοιχείο του ελεύθερου λογισμικού ανοικτού κώδικα στο δικό του προϊόν με ψηφιακά στοιχεία, πρέπει να επιδεικνύει δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5.

Παράδειγμα 33: Μη κερδοσκοπική οντότητα που έχει συσταθεί με τρόπο που διασφαλίζει ότι όλα τα έσοδα μετά την κάλυψη του κόστους χρησιμοποιούνται για την επίτευξη μη κερδοσκοπικών στόχων δημοσιεύει πακέτο ανάπτυξης λογισμικού (SDK) ελεύθερου λογισμικού ανοικτού κώδικα και διασφαλίζει τη διαρκή συντήρησή του. Το πακέτο ανάπτυξης λογισμικού διανέμεται ανοικτά και είναι ελεύθερα διαθέσιμο σε όλους για πρόσβαση, χρήση, τροποποίηση και αναδιανομή. Η χρηματοδότηση παρέχεται μέσω συνδρομών μελών που καταβάλλονται στη μη κερδοσκοπική οντότητα και οι προγραμματιστές που απασχολούνται από τους οργανισμούς-μέλη συνεισφέρουν κώδικα και άλλους πόρους για την ανάπτυξη του πακέτου ανάπτυξης λογισμικού. Οι κατασκευαστές χρησιμοποιούν το πακέτο ανάπτυξης λογισμικού ως δομοστοιχείο για την κατασκευή άλλων προϊόντων με ψηφιακά στοιχεία.

Η μη κερδοσκοπική οντότητα που δημοσιεύει το εν λόγω πακέτο ανάπτυξης λογισμικού είναι ο υποστηρικτής του. Τα μέλη του ιδρύματος δεν είναι υπεύθυνα για τη συμμόρφωση του πακέτου ανάπτυξης λογισμικού με τον κανονισμό για την κυβερνοανθεκτικότητα. Όταν οι κατασκευαστές χρησιμοποιούν το πακέτο ανάπτυξης λογισμικού για την κατασκευή του δικού τους προϊόντος με ψηφιακά στοιχεία, πρέπει να επιδεικνύουν δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5.

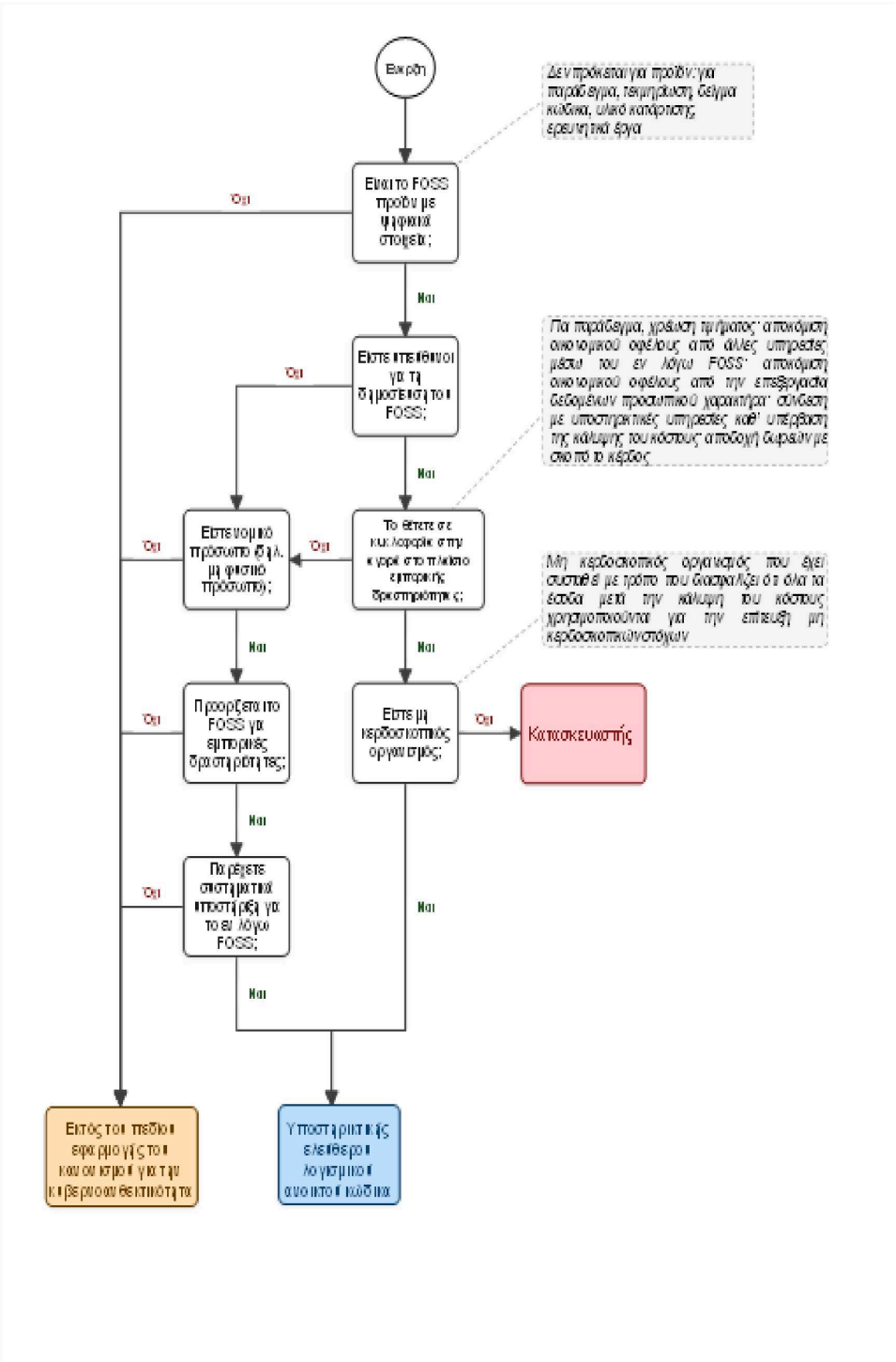
Παράδειγμα 34: Μεμονωμένος προγραμματιστής δημοσιεύει βιβλιοθήκη ελεύθερου λογισμικού ανοικτού κώδικα σε δημόσιο αποθετήριο πακέτων για δεδομένη γλώσσα προγραμματισμού και τη συντηρεί ενεργά. Στην τεκμηρίωση του πακέτου, ο προγραμματιστής προσθέτει έναν σύνδεσμο για τη συγκέντρωση δωρεών. Κατασκευαστής καταφορτώνει δωρεάν την εν λόγω βιβλιοθήκη από το αποθετήριο και την ενσωματώνει στο δικό του προϊόν με ψηφιακά στοιχεία.

Ο μεμονωμένος προγραμματιστής και το αποθετήριο πακέτων δεν υπέχουν υποχρεώσεις σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα. Ο κατασκευαστής που ενσωματώνει τη βιβλιοθήκη πρέπει να επιδεικνύει τη δέουσα επιμέλεια σύμφωνα με το άρθρο 13 παράγραφος 5.

([15]) Εκτός εάν η εταιρεία Α είναι μη κερδοσκοπική οντότητα που έχει συσταθεί με τρόπο που διασφαλίζει ότι όλα τα έσοδα μετά την κάλυψη του κόστους χρησιμοποιούνται για την επίτευξη μη κερδοσκοπικών στόχων και, ως εκ τούτου, είναι ο υποστηρικτής του εν λόγω ελεύθερου λογισμικού ανοικτού κώδικα.

Διάγραμμα 1

Απλοποιημένο διάγραμμα ροής για την κάλυψη ελεύθερου λογισμικού ανοικτού κώδικα από τον κανονισμό για την κυβερνοανθεκτικότητα



4. **ΟΥΣΙΑΣΤΙΚΕΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ ΚΑΙ ΑΝΤΑΛΛΑΚΤΙΚΑ**

90. Στο άρθρο 3 σημείο 30) του κανονισμού για την κυβερνοανθεκτικότητα ορίζεται η «ουσιαστική τροποποίηση» ως αλλαγή στο προϊόν με ψηφιακά στοιχεία μετά τη θέση του σε κυκλοφορία στην αγορά, η οποία i) επηρεάζει τη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία προς τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι μέρος Ι· ή ii) έχει ως αποτέλεσμα τροποποίηση του προβλεπόμενου σκοπού για τον οποίο έχει αξιολογηθεί το προϊόν με ψηφιακά στοιχεία.

91. Η έννοια της ουσιαστικής τροποποίησης είναι σημαντική για την εξακρίβωση των υποχρεώσεων σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα σε σειρά περιπτώσεων, συμπεριλαμβανομένων των ακόλουθων:

α) σύμφωνα με το άρθρο 21, εισαγωγέας ή διανομέας που τροποποιεί ουσιωδώς προϊόν με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά θεωρείται ο κατασκευαστής του·

β) σύμφωνα με το άρθρο 22, κάθε φυσικό ή νομικό πρόσωπο που πραγματοποιεί ουσιαστική τροποποίηση προϊόντος με ψηφιακά στοιχεία και το διαθέτει στην αγορά θεωρείται ο κατασκευαστής του·

γ) σύμφωνα με το άρθρο 69 παράγραφος 2, κάθε φυσικό ή νομικό πρόσωπο που πραγματοποιεί ουσιαστική τροποποίηση μετά τις 11 Δεκεμβρίου 2027 προϊόντος με ψηφιακά στοιχεία που έχει τεθεί σε κυκλοφορία στην αγορά πριν από τις 11 Δεκεμβρίου 2027 και το θέτει σε κυκλοφορία στην αγορά θεωρείται ο κατασκευαστής του·

δ) όσον αφορά τους κατασκευαστές προϊόντων με ψηφιακά στοιχεία που τίθενται σε κυκλοφορία στην αγορά μετά τις 11 Δεκεμβρίου 2027, προκειμένου να προσδιοριστεί αν ένα προϊόν με ψηφιακά στοιχεία απαιτείται να υποβληθεί σε νέα διαδικασία αξιολόγησης της συμμόρφωσης λόγω αλλαγών που πραγματοποιήθηκαν μετά την εν λόγω ημερομηνία, ιδίως υπό το πρίσμα του επαναληπτικού χαρακτήρα της ανάπτυξης λογισμικού.

92. Ως εκ τούτου, είναι σημαντικό να παρέχεται καθοδήγηση που θα βοηθά τους οικονομικούς φορείς να κατανοούν πότε οι τροποποιήσεις υλισμικού ή λογισμικού μπορούν να χαρακτηριστούν ως ουσιαστικές τροποποιήσεις.

4.1. **Υλικές επισκευές**

93. Όπως αναφέρεται στην αιτιολογική σκέψη 42 του κανονισμού για την κυβερνοανθεκτικότητα «[ό]ταν προϊόν με ψηφιακά στοιχεία υπόκειται σε "ανακατασκευή", "συντήρηση" και "επισκευή" προϊόντος με ψηφιακά στοιχεία, όπως ορίζεται στο άρθρο 2 σημεία 18), 19) και 20) του κανονισμού (ΕΕ) 2024/1781 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, τούτο δεν συνεπάγεται κατ' ανάγκη ουσιαστική τροποποίηση του προϊόντος, για παράδειγμα εάν ο προβλεπόμενος σκοπός και οι λειτουργίες δεν αλλάξουν και το επίπεδο κινδύνου παραμένει αμετάβλητο. Ωστόσο, η αναβάθμιση ενός προϊόντος με ψηφιακά στοιχεία από τον κατασκευαστή ενδέχεται να οδηγήσει σε αλλαγές στον σχεδιασμό και την ανάπτυξη του εν λόγω προϊόντος και, ως εκ τούτου, ενδέχεται να επηρεάσει τον προβλεπόμενο σκοπό και τη συμμόρφωση προς τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό». Αυτό συνάδει με το σημείο 2.1 του Γαλάζιου Οδηγού, όπου υπενθυμίζεται ότι «Προϊόν το οποίο έχει υποστεί σημαντικές αλλαγές ή επισκευές αφού έχει τεθεί σε λειτουργία πρέπει να θεωρείται νέο προϊόν αν: i) οι αρχικές επιδόσεις του, ο προορισμός ή ο τύπος του τροποποιούνται, χωρίς αυτό να έχει προβλεφθεί στην αρχική εκτίμηση κινδύνου· ii) η φύση της πηγής κινδύνου έχει μεταβληθεί ή το επίπεδο του κινδύνου έχει αυξηθεί σε σχέση με τη σχετική ενωσιακή νομοθεσία εναρμόνισης· και iii) το προϊόν καθίσταται διαθέσιμο (ή τίθεται σε λειτουργία εάν το πεδίο εφαρμογής της ισχύουσας νομοθεσίας καλύπτει επίσης τη θέση σε λειτουργία). Αυτό πρέπει να αξιολογείται κατά περίπτωση και ιδίως σε σχέση με τον σκοπό της νομοθεσίας και τον τύπο των προϊόντων που καλύπτονται από την εν λόγω νομοθεσία».

94. Οι εργασίες ανακατασκευής, συντήρησης ή επισκευής που έχουν ως αποτέλεσμα υλικές τροποποιήσεις προϊόντων με ψηφιακά στοιχεία που έχουν ήδη τεθεί σε κυκλοφορία στην αγορά δεν ισοδυναμούν κατ' ανάγκη με ουσιαστικές τροποποιήσεις. Ως εκ τούτου, θα πρέπει να διενεργείται κατά περίπτωση αξιολόγηση, ώστε να εξακριβώνεται αν η εν λόγω υλική τροποποίηση επηρεάζει τη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία προς τις ουσιώδεις απαιτήσεις του παραρτήματος Ι μέρος Ι ή έχει ως αποτέλεσμα τροποποίηση του προβλεπόμενου σκοπού του προϊόντος που καλύπτεται από την εκτίμηση κινδύνων κυβερνοασφάλειας.

95. Η αντικατάσταση ελαττωματικών εξαρτημάτων ή φθαρμένων αντικειμένων από εξαρτήματα που έχουν καλύτερες επιδόσεις (π.χ. λόγω τεχνικής προόδου ή επειδή το παλαιό εξάρτημα δεν παράγεται πλέον) δεν συνεπάγεται από μόνη της ουσιαστική τροποποίηση του επισκευασμένου προϊόντος με ψηφιακά στοιχεία. Αυτό συμβαίνει μόνο εάν οι επιδόσεις αλλάξουν ή ο τρόπος λειτουργίας του επισκευασμένου προϊόντος με ψηφιακά στοιχεία i) επηρεάζει τη συμμόρφωσή του προς τις ουσιώδεις απαιτήσεις ή ii) έχει ως αποτέλεσμα τροποποίηση του προβλεπόμενου σκοπού που δεν καλυπτόταν από την εκτίμηση κινδύνων.

Παράδειγμα 35: Ο κατασκευαστής διακομιστή υπολογιστών εκτελεί εργασία επισκευής, αντικαθιστώντας μια ελαττωματική μνήμη RAM με μια νέα, με καλύτερες επιδόσεις. Η συμμόρφωση του διακομιστή με τις ουσιώδεις απαιτήσεις δεν επηρεάζεται. Οι επιδόσεις του διακομιστή βελτιώνονται, αλλά οι νέες επιδόσεις του παραμένουν εντός της προβλεπόμενης χρήσης του διακομιστή, όπως αυτή ελήφθη υπόψη στην εκτίμηση κινδύνων κυβερνοασφάλειας. Ο διακομιστής υπολογιστών δεν θεωρείται ότι έχει υποστεί ουσιαστική τροποποίηση.

4.2. **Ανταλλακτικά**

96. Το άρθρο 2 παράγραφος 6 του κανονισμού για την κυβερνοανθεκτικότητα ορίζει ότι τα ανταλλακτικά που προορίζονται για την αντικατάσταση πανομοιότυπων δομοστοιχείων και κατασκευάζονται σύμφωνα με τις ίδιες προδιαγραφές με τα εν λόγω δομοστοιχεία δεν υπόκεινται στον κανονισμό για την κυβερνοανθεκτικότητα. Στην αιτιολογική σκέψη 29 αναφέρεται περαιτέρω ότι η εξαίρεση καλύπτει τόσο τα ανταλλακτικά για προϊόντα με ψηφιακά στοιχεία που κατέστησαν διαθέσιμα πριν από την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα όσο και τα ανταλλακτικά που έχουν ήδη υποβληθεί σε διαδικασία αξιολόγησης της συμμόρφωσης, όπως ορίζεται στον κανονισμό.

97. Η εξαίρεση του άρθρου 2 παράγραφος 6 του κανονισμού για την κυβερνοανθεκτικότητα θα πρέπει να νοείται ότι εφαρμόζεται μόνο όταν το ανταλλακτικό παρέχεται ειδικά για την επισκευή ή την παράταση της ανθεκτικότητας προϊόντος με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά (πριν ή μετά τις 11 Δεκεμβρίου 2027). Όταν ένα προϊόν με ψηφιακά στοιχεία παρέχεται ως αυτόνομο προϊόν, χωρίς καμία σύνδεση με τη συντήρηση ή την επισκευή προϋπάρχοντος προϊόντος με ψηφιακά στοιχεία, τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα και δεν θα πρέπει να θεωρείται ανταλλακτικό που εμπίπτει στο πεδίο εφαρμογής του άρθρου 2 παράγραφος 6. Ο σκοπός συντήρησης ή επισκευής θα πρέπει να είναι εμφανής από το πλαίσιο της προμήθειας, για παράδειγμα μέσω της ταυτοποίησης του προϊόντος με ψηφιακά στοιχεία ή της οικογένειας προϊόντων στην παραγγελία ή την εμπορική προσφορά ή μέσω της προμήθειας μέσω διαύλων εξυπηρέτησης μετά την πώληση ή παροχής υπηρεσιών. Τα σχετικά αποδεικτικά στοιχεία θα πρέπει επίσης να παραμένουν στη διάθεση των αρχών εποπτείας της αγοράς. Το γεγονός ότι ένα προϊόν με ψηφιακά στοιχεία θα μπορούσε τεχνικά να χρησιμοποιηθεί για την αντικατάσταση ενός δομοστοιχείου δεν αρκεί από μόνο του για να το εντάξει στο πεδίο εφαρμογής της εξαίρεσης ελλείψει τέτοιων στοιχείων.

98. Ως εκ τούτου, όταν ένα ανταλλακτικό είναι πανομοιότυπο με δομοστοιχείο που περιλαμβάνεται ήδη σε προϊόν με ψηφιακά στοιχεία το οποίο είτε έχει τεθεί σε κυκλοφορία στην αγορά πριν από την ημερομηνία εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα είτε έχει τεθεί σε κυκλοφορία στην αγορά σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα, το εν λόγω ανταλλακτικό δεν υπόκειται το ίδιο στον κανονισμό για την κυβερνοανθεκτικότητα.

99. Η αξιολόγηση του αν ένα ανταλλακτικό θα πρέπει να θεωρείται πανομοιότυπο με δομοστοιχείο θα πρέπει να επικεντρώνεται στον λειτουργικό του ρόλο στο προϊόν με ψηφιακά στοιχεία και στα χαρακτηριστικά που ενδέχεται να σχετίζονται με την κυβερνοασφάλεια. Παρότι απαιτείται πάντα η διενέργεια κατά περίπτωση αξιολόγησης, οι διαφορές που δεν επηρεάζουν τα χαρακτηριστικά ασφάλειας ή το προφίλ κινδύνου κυβερνοασφάλειας του δομοστοιχείου δεν εμποδίζουν, αυτές καθαυτές, το εν λόγω ανταλλακτικό να εμπίπτει στο πεδίο εφαρμογής του άρθρου 2 παράγραφος 6 του κανονισμού για την κυβερνοανθεκτικότητα.

100. Αντιθέτως, οι διαφορές στα χαρακτηριστικά που σχετίζονται με την κυβερνοασφάλεια του δομοστοιχείου, όπως αλγόριθμοι, πρωτόκολλα, κρυπτογραφικοί μηχανισμοί, χαρακτηριστικά ελέγχου πρόσβασης ή άλλα χαρακτηριστικά σχετικά με την ασφάλεια, μπορεί να συνεπάγονται ότι το νέο εξάρτημα δεν μπορεί να θεωρηθεί πανομοιότυπο με το δομοστοιχείο που προορίζεται να αντικαταστήσει.

101. Όταν ένα ανταλλακτικό δεν είναι πανομοιότυπο με το αρχικό δομοστοιχείο, το εν λόγω ανταλλακτικό αποτελεί προϊόν με ψηφιακά στοιχεία από μόνο του και, ως εκ τούτου, υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα. Στις περιπτώσεις αυτές, η συμμόρφωση με τις ουσιώδεις απαιτήσεις πρέπει να αξιολογείται με βάση τον προβλεπόμενο σκοπό του δομοστοιχείου αντικατάστασης. Ιδιαίτερης σημασίας είναι η λειτουργία του δομοστοιχείου αντικατάστασης να διασφαλίζει τη συμβατότητα ή τη διαλειτουργικότητα με υφιστάμενο προϊόν με ψηφιακά στοιχεία, μεταξύ άλλων όταν το εν λόγω προϊόν είναι προϊόν με ψηφιακά στοιχεία που έχει τεθεί σε κυκλοφορία στην αγορά πριν από την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Όταν ορισμένες ουσιώδεις απαιτήσεις δεν μπορούν εύλογα να εκπληρωθούν λόγω του προαναφερόμενου προβλεπόμενου σκοπού ή τεχνικών περιορισμών, ο κατασκευαστής πρέπει να το αποτυπώνει αυτό στην εκτίμηση κινδύνων κυβερνοασφάλειας και να εφαρμόζει κατάλληλα εναλλακτικά ή αντισταθμιστικά μέτρα μετριασμού του κινδύνου, προκειμένου να μην υπονομεύεται η ασφάλεια του προϊόντος με ψηφιακά στοιχεία. Όπως αναλύεται επίσης στο τμήμα *2.6 Complex systems*, τόσο ο τεχνικός φάκελος όσο και οι πληροφορίες και οι οδηγίες προς τον χρήστη διαδραματίζουν καίριο ρόλο στην περιγραφή των περιορισμών που έχουν προσδιοριστεί, των σχετικών κινδύνων κυβερνοασφάλειας και των εφαρμοζόμενων μέτρων μετριασμού του κινδύνου με διαφανή τρόπο. Όπως εξηγείται στο τμήμα *4.1 Physical repairs*, η αντικατάσταση ελαττωματικών εξαρτημάτων ή φθαρμένων αντικειμένων από εξαρτήματα με καλύτερες επιδόσεις δεν συνεπάγεται από μόνη της ουσιαστική τροποποίηση του επισκευασμένου προϊόντος με ψηφιακά στοιχεία.

Παράδειγμα 36: Κατασκευαστής έχει θέσει συνδεδεμένους ελεγκτές σε κυκλοφορία στην αγορά της ΕΕ. Σε μία περίπτωση, ο ελεγκτής τέθηκε σε κυκλοφορία στην αγορά το 2026, πριν από την ημερομηνία εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Σε άλλη περίπτωση, ο ελεγκτής τέθηκε σε κυκλοφορία στην αγορά το 2028, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα. Το 2028, μια ψηφιακή μονάδα επικοινωνίας και στους δύο τύπους ελεγκτών παρουσιάζει βλάβη. Ο κατασκευαστής παρέχει ως ανταλλακτικό μονάδα αντικατάστασης που είναι πανομοιότυπη και κατασκευάζεται σύμφωνα με τις ίδιες προδιαγραφές με την αρχική μονάδα.

Και στις δύο περιπτώσεις, η μονάδα αντικατάστασης εμπίπτει στο πεδίο εφαρμογής της εξαίρεσης του άρθρου 2 παράγραφος 6. Το ίδιο το ανταλλακτικό δεν υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα, παρόλο που πρόκειται για προϊόν με ψηφιακά στοιχεία, διότι αντικαθιστά πανομοιότυπο δομοστοιχείο σε προϊόν με ψηφιακά στοιχεία. Η επισκευή δεν συνιστά ουσιαστική τροποποίηση του προϊόντος με ψηφιακά στοιχεία.

Παράδειγμα 37: Κατασκευαστής έθεσε συνδεδεμένο βιομηχανικό ελεγκτή σε κυκλοφορία στην αγορά της ΕΕ το 2026, πριν από την ημερομηνία εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα. Το 2028, ένα μικροκύκλωμα επικοινωνίας στον εν λόγω ελεγκτή παρουσιάζει βλάβη. Δεδομένου ότι ο κατασκευαστής δεν κατασκευάζει πλέον το εν λόγω μικροκύκλωμα, προμηθεύει ως ανταλλακτικό νεότερο μικροκύκλωμα με ισοδύναμη λειτουργικότητα, αλλά με διαφορετική κρυπτογραφική υλοποίηση και ενημερωμένο μηχανισμό ασφαλούς εκκίνησης, προκειμένου να διατηρηθεί η συμβατότητα και η συνεχής λειτουργία.

Στην περίπτωση αυτήν, το μικροκύκλωμα αντικατάστασης δεν μπορεί να θεωρηθεί πανομοιότυπο, καθώς οι διαφορές όσον αφορά την κρυπτογραφική υλοποίηση και τον μηχανισμό ασφαλούς εκκίνησης επηρεάζουν τις ιδιότητες κυβερνοασφάλειας του μικροκυκλώματος. Ως εκ τούτου, δεν επωφελείται από την εξαίρεση του άρθρου 2 παράγραφος 6 και αποτελεί προϊόν με ψηφιακά στοιχεία που υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα. Η συμμόρφωση του ανταλλακτικού πρέπει να αξιολογείται υπό το πρίσμα του προβλεπόμενου σκοπού του, συμπεριλαμβανομένου του ρόλου του στη διασφάλιση της διαλειτουργικότητας με το προϊόν με ψηφιακά στοιχεία που τίθεται σε κυκλοφορία στην αγορά πριν από την έναρξη εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα.

Παράδειγμα 38: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά έξυπνο ελεγκτή κτιρίου το 2028 σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα. Το 2029 η ασύρματη μονάδα του εν λόγω ελεγκτή παρουσιάζει βλάβη. Δεδομένου ότι ο κατασκευαστής δεν κατασκευάζει πλέον την εν λόγω μονάδα, προμηθεύει ως ανταλλακτικό νέα μονάδα που εκτελεί την ίδια λειτουργία χρησιμοποιώντας τα ίδια πρωτόκολλα επικοινωνίας και τους ίδιους μηχανισμούς ασφάλειας, αλλά βασίζεται σε διαφορετικό σύνολο μικροκυκλωμάτων και διαθέτει ενημερωμένο υλικολογισμικό που δεν μεταβάλλει χαρακτηριστικά που ενδέχεται να είναι σημαντικά για την κυβερνοασφάλεια.

Στην περίπτωση αυτήν, η μονάδα αντικατάστασης μπορεί να θεωρηθεί πανομοιότυπη. Ως εκ τούτου, η μονάδα επωφελείται από την εξαίρεση του άρθρου 2 παράγραφος 6 και δεν υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα.

102. Η εξαίρεση για τα ανταλλακτικά εφαρμόζεται ανεξάρτητα από το αν το ανταλλακτικό αντικαθιστά δομοστοιχείο εντός προϊόντος με ψηφιακά στοιχεία ή αν αντικαθιστά πλήρες προϊόν με ψηφιακά στοιχεία που αποτελεί το ίδιο μέρος μεγαλύτερου προϊόντος, μεταξύ άλλων όταν το εν λόγω μεγαλύτερο προϊόν με ψηφιακά στοιχεία αποτελείται από διάφορα ενσωματωμένα δομοστοιχεία, υπό την προϋπόθεση ότι το ανταλλακτικό παρέχεται ειδικά ως ανταλλακτικό, όπως εξηγείται στα προηγούμενα σημεία.

Παράδειγμα 39: Το 2027 ένας κατασκευαστής θέτει σε κυκλοφορία στην αγορά βιομηχανικό σύστημα αυτοματοποίησης που ενσωματώνει προγραμματιζόμενο λογικό ελεγκτή (στο εξής: PLC) ως ένα από τα δομοστοιχεία του. Το 2031 η κεντρική μονάδα επεξεργασίας (CPU) του PLC παρουσιάζει βλάβη. Ο κατασκευαστής προσφέρει δύο επιλογές επισκευής: i) την προμήθεια μονάδας CPU αντικατάστασης, η οποία μπορεί να θεωρηθεί πανομοιότυπη με την κεντρική μονάδα επεξεργασίας που εγκαταστάθηκε αρχικά· ή ii) την προμήθεια πλήρους PLC αντικατάστασης, το οποίο μπορεί να θεωρηθεί πανομοιότυπο με τον PLC που είχε αρχικά εγκατασταθεί. Σε κάθε περίπτωση, το στοιχείο αντικατάστασης παρέχεται μέσω του διαύλου εξυπηρέτησης μετά την πώληση του κατασκευαστή ως ανταλλακτικό και το βιομηχανικό σύστημα αυτοματοποίησης για το οποίο προορίζεται το ανταλλακτικό ταυτοποιείται σαφώς. Και στις δύο περιπτώσεις, η αντικατάσταση εμπίπτει στο πεδίο εφαρμογής της απαλλαγής του άρθρου 2 παράγραφος 6, είτε η αντικατάσταση αφορά δομοστοιχείο του PLC είτε το PLC στο σύνολό του.

4.3. **Ενημερώσεις λογισμικού ως ουσιώδεις τροποποιήσεις**

103. Η ανάπτυξη λογισμικού έχει επαναληπτικό χαρακτήρα, καθώς τα προϊόντα λογισμικού με ψηφιακά στοιχεία που έχουν ήδη τεθεί σε κυκλοφορία στην αγορά ενημερώνονται συχνά και διαρκώς. Στο πλαίσιο αυτό, είναι χρήσιμο να παρασχεθεί περισσότερη καθοδήγηση προκειμένου να διαπιστώνεται πότε το λογισμικό πρέπει να θεωρείται ουσιωδώς τροποποιημένο. Σκοπός της εν λόγω καθοδήγησης είναι ιδίως να βοηθήσει τους κατασκευαστές προϊόντων λογισμικού με ψηφιακά στοιχεία που πραγματοποιούν αλλαγές στα δικά τους προϊόντα να προσδιορίζουν κατά πόσο οι αλλαγές αυτές ισοδυναμούν με ουσιαστική τροποποίηση.

104. Στην αιτιολογική σκέψη 39 αναφέρεται ότι ένα προϊόν με ψηφιακά στοιχεία τροποποιείται ουσιωδώς όταν μια αλλαγή μεταβάλλει το επίπεδο του κινδύνου κυβερνοασφάλειας και όταν ο εν λόγω τροποποιημένος ή πρόσθετος κίνδυνος δεν έχει ληφθεί υπόψη από τον κατασκευαστή στην εκτίμηση κινδύνων του και, κατά συνέπεια, στην εφαρμογή των ουσιωδών απαιτήσεων. Ως εκ τούτου, ο κατασκευαστής θα πρέπει να αξιολογεί, κατά περίπτωση, αν μια ενημέρωση λογισμικού δημιουργεί νέους ή αυξημένους κινδύνους κυβερνοασφάλειας και αν οι κίνδυνοι αυτοί έχουν ήδη αντιμετωπιστεί στην εκτίμηση κινδύνων που διενεργεί.

105. Όταν ένας κατασκευαστής εισάγει νέες λειτουργίες σε ένα προϊόν με ψηφιακά στοιχεία που οδηγούν σε αλλαγή της προβλεπόμενης χρήσης του προϊόντος στο σύνολό του, είναι πιθανό ο κατασκευαστής να μην έλαβε υπόψη τις εν λόγω αλλαγές στην εκτίμηση κινδύνων του. Σε τέτοιες περιπτώσεις, η αλλαγή μπορεί γενικά να χαρακτηριστεί ως ουσιαστική τροποποίηση.

Παράδειγμα 40: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά πίνακα εργαλείων που συλλέγει δεδομένα από μηχανήματα και εμφανίζει τάσεις και ειδοποιήσεις, χωρίς να έχει τη δυνατότητα να ελέγχει τα εν λόγω μηχανήματα. Στη συνέχεια, ο κατασκευαστής αναπτύσσει νέα έκδοση του εν λόγω πίνακα εργαλείων, εισάγοντας λειτουργίες που του επιτρέπουν να ελέγχει τα μηχανήματα, μεταξύ άλλων ρυθμίζοντας τις παραμέτρους λειτουργίας και επανεκκινώντας τα μηχανήματα μετά από καταστάσεις βλάβης. Ως αποτέλεσμα αυτών των αλλαγών, η προβλεπόμενη χρήση του πίνακα εργαλείων έχει εξελιχθεί πέραν των όσων προβλέπονταν στην εκτίμηση κινδύνων, μεταβαίνοντας από εργαλείο επίγνωσης της κατάστασης σε προϊόν με ψηφιακά στοιχεία που προορίζεται για την άσκηση επιχειρησιακού ελέγχου σε άλλες συσκευές. Ως εκ τούτου, ο πίνακας εργαλείων έχει τροποποιηθεί ουσιωδώς.

Παράδειγμα 41: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά εφαρμογή λογισμικού για καταναλωτές που προορίζεται για την οργάνωση και την εμφάνιση δεδομένων προσωπικού χαρακτήρα, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή έγγραφα, και για την υποστήριξη βασικών λειτουργιών αναζήτησης και φιλτραρίσματος. Στη συνέχεια, ο κατασκευαστής εισάγει ενημέρωση που επιτρέπει στην εφαρμογή να αναλύει αυτόματα το περιεχόμενο των χρηστών, προκειμένου να δημιουργεί προφίλ συμπεριφοράς και να λαμβάνει αυτοματοποιημένες αποφάσεις που επηρεάζουν την προτεραιοποίηση, την καταστολή ή τη σύσταση περιεχομένου χωρίς παρέμβαση του χρήστη. Ως αποτέλεσμα αυτής της αλλαγής, ο προβλεπόμενος σκοπός του λογισμικού μετατοπίζεται από εργαλείο διαχείρισης πληροφοριών ελεγχόμενο από τον χρήστη σε αυτοματοποιημένο σύστημα λήψης αποφάσεων, το οποίο δεν προβλεπόταν στην εκτίμηση κινδύνων. Ως εκ τούτου, η εφαρμογή έχει τροποποιηθεί ουσιωδώς.

106. Ταυτόχρονα, ωστόσο, είναι πιθανό ένας κατασκευαστής να εισαγάγει σταδιακά νέες λειτουργίες που περιλαμβάνονται ήδη στην εκτίμηση κινδύνων του ή οι οποίες, αυτές καθ' εαυτές, δεν μεταβάλλουν το προφίλ κινδύνου κυβερνοασφάλειας του προϊόντος με ψηφιακά στοιχεία. Αυτό μπορεί να συμβαίνει, για παράδειγμα, όταν ο κατασκευαστής έχει προβλέψει την ανάπτυξη των εν λόγω λειτουργικοτήτων, έχει ήδη περιγράψει και αξιολογήσει τους σχετικούς κινδύνους και έχει εφαρμόσει κατάλληλα μέτρα μετριασμού για τη διασφάλιση της συνεχούς συμμόρφωσης με τις ουσιώδεις απαιτήσεις. Αυτό μπορεί επίσης να συμβαίνει όταν οι νέες λειτουργίες δεν εφαρμόζουν αλλαγές που δημιουργούν νέους ή αυξημένους κινδύνους. Ως εκ τούτου, οι ενημερώσεις αυτού του είδους δεν θα πρέπει να θεωρούνται ουσιαστικές τροποποιήσεις, καθώς δεν αυξάνουν τον κίνδυνο κυβερνοασφάλειας και, κατά συνέπεια, δεν μεταβάλλουν την εφαρμογή των ουσιωδών απαιτήσεων.

Παράδειγμα 42: Εφαρμογή ανταλλαγής μηνυμάτων κυκλοφορεί αρχικά με λειτουργία που περιορίζεται στην ανταλλαγή μηνυμάτων ενός προς έναν. Η εκτίμηση κινδύνων του κατασκευαστή καλύπτει τη μεταγενέστερη εισαγωγή της ομαδικής αποστολής μηνυμάτων, συμπεριλαμβανομένης, για παράδειγμα, της αυξημένης πολυπλοκότητας της δρομολόγησης μηνυμάτων. Σε μεταγενέστερη ενημέρωση, ο κατασκευαστής προσθέτει μια λειτουργία ομαδικής συνομιλίας μαζί με τα στοιχεία ελέγχου διαχειριστή και τα εργαλεία ελέγχου που είχαν ήδη προβλεφθεί και αξιολογηθεί στον αρχικό σχεδιασμό. Η ενημέρωση εφαρμόζει λειτουργίες που εμπίπτουν στο πεδίο εφαρμογής της αρχικής προβλεπόμενης χρήσης και της εκτίμησης κινδύνων. Ως εκ τούτου, η εφαρμογή ανταλλαγής μηνυμάτων δεν έχει τροποποιηθεί ουσιωδώς.

Παράδειγμα 43: Σύστημα παρακολούθησης της παραγωγής τίθεται σε κυκλοφορία στην αγορά με ενεργοποιημένους πίνακες εργαλείων μόνο για ανάγνωση, ενώ στην αρχιτεκτονική του συστήματος υπάρχουν λειτουργίες αυτοματοποιημένου ελέγχου, οι οποίες, ωστόσο, παραμένουν απενεργοποιημένες. Η εκτίμηση κινδύνων του κατασκευαστή καλύπτει ρητά τη μελλοντική ενεργοποίηση αυτοματοποιημένων βρόχων ελέγχου, συμπεριλαμβανομένων των κινδύνων κυβερνοασφάλειας που συνδέονται με τον έλεγχο κλειστού βρόχου, καθώς και διασφαλίσεις όπως οι μηχανισμοί παράκαμψης από τον χειριστή και οι στάσεις ασφαλείας (fail-safe). Σε μεταγενέστερη ενημέρωση, ο κατασκευαστής ενεργοποιεί τα χαρακτηριστικά αυτοματοποιημένου ελέγχου και τις διασφαλίσεις όπως αξιολογήθηκαν αρχικά. Ως εκ τούτου, το σύστημα παρακολούθησης της παραγωγής δεν έχει τροποποιηθεί ουσιωδώς.

107. Αντιθέτως, ακόμα και περιορισμένες ή φαινομενικά ήσσονος σημασίας νέες λειτουργίες ενδέχεται να ενέχουν σημαντικούς κινδύνους κυβερνοασφάλειας που επηρεάζουν τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις. Ως εκ τούτου, η αξιολόγηση της ουσιαστικής τροποποίησης δεν θα πρέπει να βασίζεται στην κλίμακα ή την πολυπλοκότητα της αλλαγής, αλλά στις δυνητικές αρνητικές επιπτώσεις της στο προφίλ κινδύνου κυβερνοασφάλειας του προϊόντος με ψηφιακά στοιχεία και, κατά συνέπεια, στην εφαρμογή των ουσιωδών απαιτήσεων.

Παράδειγμα 44: Κατασκευαστής εισάγει ενημέρωση σε εφαρμογή λογισμικού προσθέτοντας λειτουργία διατήρησης της σύνδεσης η οποία αποθηκεύει αδειοδοτικά επαλήθευσης ταυτότητας σε τοπικό επίπεδο για βελτιωμένη διευκόλυνση του χρήστη. Μολονότι η λειτουργία έχει περιορισμένο πεδίο εφαρμογής, δημιουργεί νέους κινδύνους που σχετίζονται με την κλοπή αδειοδοτικού, τη μη εξουσιοδοτημένη πρόσβαση και την υφαρπαγή περιόδου λειτουργίας, οι οποίοι δεν ελήφθησαν υπόψη στην εκτίμηση κινδύνων. Ως εκ τούτου, η ενημέρωση επηρεάζει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις. Η εφαρμογή λογισμικού έχει τροποποιηθεί ουσιωδώς.

Παράδειγμα 45: Κατασκευαστής προσθέτει νέο χαρακτηριστικό καταγραφής και διαγνωστικού ελέγχου σε υφιστάμενο προϊόν λογισμικού με ψηφιακά στοιχεία, το οποίο επιτρέπει την εξαγωγή λεπτομερών αρχείων καταγραφής συστήματος για σκοπούς επίλυσης προβλημάτων. Μολονότι η λειτουργία φαίνεται ότι είναι ήσσονος σημασίας, έχει ως αποτέλεσμα τη συλλογή και αποθήκευση ευαίσθητων επιχειρησιακών δεδομένων σε μη κρυπτογραφημένο μορφότυπο, κάτι που δημιουργεί κινδύνους έκθεσης δεδομένων που δεν είχαν προηγουμένως αξιολογηθεί ή μετριαστεί. Ως εκ τούτου, η αλλαγή μπορεί να έχει σημαντικές επιπτώσεις στο προφίλ κινδύνου κυβερνοασφάλειας του προϊόντος με ψηφιακά στοιχεία. Το προϊόν λογισμικού με ψηφιακά στοιχεία έχει τροποποιηθεί ουσιωδώς.

108. Σύμφωνα με την αιτιολογική σκέψη 39 του κανονισμού για την κυβερνοανθεκτικότητα, οι ενημερώσεις ασφαλείας δεν πρέπει γενικά να θεωρούνται ουσιαστικές τροποποιήσεις, δεδομένου ότι πρωταρχικός σκοπός τους είναι η μείωση του επιπέδου κινδύνου κυβερνοασφάλειας που συνδέεται με το προϊόν με ψηφιακά στοιχεία. Ως εκ τούτου, μια ενημέρωση ασφαλείας που δεν τροποποιεί τον επιδιωκόμενο σκοπό του εν λόγω προϊόντος και δεν δημιουργεί νέους κινδύνους κυβερνοασφάλειας δεν θα πρέπει να θεωρείται ουσιαστική τροποποίηση, ακόμα και όταν η εν λόγω ενημέρωση μπορεί να εισαγάγει σημαντικές τεχνικές αλλαγές. Σε αυτό το πλαίσιο περιλαμβάνεται η περίπτωση κατά την οποία ορισμένες λειτουργίες τροποποιούνται ή περιορίζονται αποκλειστικά με σκοπό τον μετριασμό των ευπαθειών που έχουν εντοπιστεί και τη διασφάλιση της συνεχούς συμμόρφωσης προς τις ουσιώδεις απαιτήσεις.

Παράδειγμα 46: Κατασκευαστής χρησιμοποιεί ενημέρωση ασφαλείας για την αντιμετώπιση ευπάθειας στη βάση κώδικα προϊόντος με ψηφιακά στοιχεία, μέσω της διόρθωσης σφάλματος επικύρωσης εισόδου που μπορεί να οδηγήσει σε υπερχείλιση προσωρινής μνήμης ή μέσω της διόρθωσης λογικού ελαττώματος που επιτρέπει την παράκαμψη της επαλήθευσης ταυτότητας μέσω εσφαλμένης επικύρωσης αδειοδοτικού περιόδου λειτουργίας. Η ενημέρωση τροποποιεί την εσωτερική εφαρμογή του λογισμικού χωρίς να επηρεάζει τον προβλεπόμενο σκοπό του εν λόγω προϊόντος ή να δημιουργεί νέα έκθεση. Η ενημέρωση αυτή αποσκοπεί αποκλειστικά στη μείωση των κινδύνων κυβερνοασφάλειας. Η ενημέρωση ασφαλείας δεν θα πρέπει να θεωρείται ουσιαστική τροποποίηση.

Παράδειγμα 47: Κατασκευαστής εισάγει ενημέρωση ασφαλείας που ενισχύει τις υφιστάμενες διαμορφώσεις ασφαλείας, όπως αυστηροποίηση των κανόνων του τείχους προστασίας, απενεργοποίηση αχρησιμοποίητων θυρών δικτύου, αλλαγή των προεπιλεγμένων πολιτικών για τους κωδικούς πρόσβασης του διαχειριστή ή υποχρεωτική πολυπαραγοντική επαλήθευση ταυτότητας ενώ η εν λόγω λειτουργία ήταν ήδη διαθέσιμη ή προβλεπόμενη. Μολονότι η ενημέρωση μπορεί να επηρεάζει τον τρόπο με τον οποίο οι χρήστες διαμορφώνουν το προϊόν με ψηφιακά στοιχεία ή έχουν πρόσβαση σε αυτό, δεν μεταβάλλει τον επιδιωκόμενο σκοπό του και χρησιμεύει αποκλειστικά για την ενίσχυση της κατάστασης κυβερνοασφάλειάς του. Η ενημέρωση ασφαλείας δεν θα πρέπει να θεωρείται ουσιαστική τροποποίηση.

Παράδειγμα 48: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά προϊόν λογισμικού με ψηφιακά στοιχεία που εξασφαλίζει επικοινωνίες με τη χρήση διαμορφώσιμου πλαισίου κρυπτογράφησης που υποστηρίζει πολλαπλούς κρυπτογραφικούς αλγόριθμους και μεγέθη κλειδιών, όπως περιγράφονται στον τεχνικό φάκελο και στην εκτίμηση κινδύνων του προϊόντος. Η εκτίμηση κινδύνων καλύπτει όλες τις κρυπτογραφικές επιλογές που παρέχονται στο προϊόν με ψηφιακά στοιχεία και προβλέπει τη μελλοντική κατάργηση ορισμένων αλγορίθμων. Η εκτίμηση κινδύνων περιλαμβάνει επίσης μέτρα μετριασμού, όπως η κρυπτογραφική ευελιξία, η εσωτερική διαχείριση κλειδιών και οι δοκιμές συμβατότητας. Ανταποκρινόμενος στις εξελισσόμενες κρυπτογραφικές κατευθυντήριες γραμμές, ο κατασκευαστής χρησιμοποιεί ενημέρωση ασφαλείας που απενεργοποιεί έναν καταργημένο αλγόριθμο και ενεργοποιεί μια ισχυρότερη, ήδη υποστηριζόμενη εναλλακτική λύση, χωρίς να εισάγει νέες εξωτερικές εξαρτήσεις ή να μεταβάλλει τις ροές δεδομένων. Δεδομένου ότι η ενημέρωση εφαρμόζει μέτρο ασφάλειας που προβλεπόταν και αξιολογήθηκε στο πλαίσιο του αρχικού σχεδιασμού και δεν δημιουργεί νέους κινδύνους κυβερνοασφάλειας, η ενημέρωση ασφαλείας δεν θα πρέπει να θεωρείται ουσιαστική τροποποίηση.

109. Αντιθέτως, μια ενημέρωση ασφαλείας μπορεί να χαρακτηριστεί ως ουσιαστική τροποποίηση όταν, παρά τον στόχο της όσον αφορά την ασφάλεια, έχει ως αποτέλεσμα την τροποποίηση του επιδιωκόμενου σκοπού του προϊόντος με ψηφιακά στοιχεία πέραν του αρχικά προβλεπόμενου ή όταν δημιουργεί νέους ή αυξημένους κινδύνους για την κυβερνοασφάλεια. Αυτό μπορεί να συμβαίνει, για παράδειγμα, όταν μια ενημέρωση μεταβάλλει σε σημαντικό βαθμό τα όρια ή τη δομή εξάρτησης του εν λόγω προϊόντος με τρόπο που δεν προβλέπεται στην εκτίμηση κινδύνων, π.χ. μεταβάλλοντας σε σημαντικό βαθμό τις ροές δεδομένων ή προσθέτοντας νέες εξωτερικά προσβάσιμες διεπαφές.

Παράδειγμα 49: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά προϊόν λογισμικού με ψηφιακά στοιχεία που προορίζεται να παρέχει κρυπτογράφηση τοπικών αρχείων για δεδομένα που είναι αποθηκευμένα στη συσκευή ενός χρήστη, επιτρέποντας στους χρήστες να κρυπτογραφούν και να αποκρυπτογραφούν αρχεία κατόπιν σχετικού αιτήματος. Μετά τον εντοπισμό ευπάθειας στη ροή εργασιών κρυπτογράφησης, ο κατασκευαστής εφαρμόζει ενημέρωση ασφαλείας που καταργεί τη λειτουργία τοπικής κρυπτογράφησης και, αντ' αυτού, απαιτεί όλα τα αρχεία να μεταφορτώνονται, να αποθηκεύονται και να υποβάλλονται σε επεξεργασία από υπηρεσία εξ αποστάσεως κρυπτογράφησης την οποία διαχειρίζεται ο κατασκευαστής. Ως αποτέλεσμα αυτής της αλλαγής, το προϊόν με ψηφιακά στοιχεία δεν εκτελεί πλέον τοπική κρυπτογράφηση όπως προβλεπόταν αρχικά, αλλά λειτουργεί ως υπηρεσία εξ αποστάσεως κρυπτογράφησης και επεξεργασίας δεδομένων. Μολονότι η ενημέρωση εισάγεται για λόγους ασφαλείας, μεταβάλλει ριζικά τον επιδιωκόμενο σκοπό του εν λόγω προϊόντος με τρόπο που δεν προβλέπεται στην εκτίμηση κινδύνων και, ως εκ τούτου, μπορεί να χαρακτηριστεί ως ουσιαστική τροποποίηση.

Παράδειγμα 50: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά προϊόν λογισμικού με ψηφιακά στοιχεία που βασίζεται σε καθιερωμένο πρωτόκολλο κρυπτογράφησης και σε εσωτερικά διαχειριζόμενο κύκλο ζωής κλειδιών για την ασφάλεια των επικοινωνιών μεταξύ των δομοστοιχείων του προϊόντος με ψηφιακά στοιχεία. Ανταποκρινόμενος σε νεοεντοπισθείσες κρυπτογραφικές αδυναμίες, ο κατασκευαστής εισάγει ενημέρωση ασφαλείας που αντικαθιστά τον υφιστάμενο μηχανισμό κρυπτογράφησης με διαφορετικό πρωτόκολλο που απαιτεί τη χρήση εξωτερικής υπηρεσίας διαχείρισης κλειδιών, την οποία διαχειρίζεται τρίτο μέρος. Ως αποτέλεσμα αυτής της αλλαγής, οι εξαρτήσεις και οι ροές δεδομένων του προϊόντος με ψηφιακά στοιχεία τροποποιούνται ουσιαστικά, με την εισαγωγή νέων εξωτερικών διεπαφών και την εξάρτηση από υπηρεσίες τρίτων που δεν λαμβάνονται υπόψη στην εκτίμηση κινδύνων. Μολονότι η ενημέρωση επικεντρώνεται στην ασφάλεια, δημιουργεί νέους κινδύνους για την κυβερνοασφάλεια και, ως εκ τούτου, μπορεί να χαρακτηριστεί ως ουσιαστική τροποποίηση.

110. Όπως αναφέρεται στο σημείο 104 ανωτέρω, το αν μια ενημέρωση λογισμικού αποτελεί ουσιαστική τροποποίηση θα πρέπει να αξιολογείται κατά περίπτωση. Κατά τη διενέργεια της εν λόγω αξιολόγησης, οι κατασκευαστές μπορούν να εξετάζουν, με μη εξαντλητικό τρόπο, αν η ενημέρωση λογισμικού:

α) δημιουργεί νέους φορείς απειλών, όπως πρόσθετες διεπαφές, διαύλους επικοινωνίας, περιβάλλοντα εκτέλεσης ή εξωτερικές εξαρτήσεις μέσω των οποίων θα μπορούσαν να υλοποιηθούν απειλές·

β) καθιστά δυνατά νέα σενάρια επιθέσεων, συμπεριλαμβανομένων, για παράδειγμα, νέων τρόπων με τους οποίους θα μπορούσε ευλόγως να προκύψει μη εξουσιοδοτημένη πρόσβαση, χειραγώγηση, παρέμβαση ή κακή χρήση του προϊόντος με ψηφιακά στοιχεία ή των δεδομένων που υποβάλλονται σε επεξεργασία από αυτό·

γ) μεταβάλλει την πιθανότητα σεναρίων επιθέσεων που είχαν προσδιοριστεί προηγουμένως, για παράδειγμα μειώνοντας την προσπάθεια ή την εμπειρογνωσία που απαιτείται για την εκμετάλλευσή τους, αυξάνοντας την έκθεση σε μη αξιόπιστους παράγοντες ή αποδυναμώνοντας τις υφιστάμενες διασφαλίσεις·

δ) μεταβάλλει τις δυνητικές επιπτώσεις σεναρίων επιθέσεων που είχαν προσδιοριστεί προηγουμένως, συμπεριλαμβανομένων, για παράδειγμα, του πεδίου εφαρμογής των επηρεαζόμενων δεδομένων ή λειτουργιών, της σοβαρότητας των επιχειρησιακών συνεπειών, των συνεπειών για την ασφάλεια ή των οικονομικών συνεπειών ή της ικανότητας εντοπισμού, περιορισμού ή ανάκαμψης από περιστατικό.

111. Σε ορισμένες περιπτώσεις, η ενημέρωση λογισμικού δεν δημιουργεί νέους φορείς απειλής, δεν καθιστά δυνατά νέα σενάρια επίθεσης και δεν μεταβάλλει σε σημαντικό βαθμό την πιθανότητα ή τις επιπτώσεις των σεναρίων επίθεσης που είχαν προσδιοριστεί προηγουμένως. Αυτό μπορεί να υποδεικνύει ότι η ενημέρωση δεν δημιουργεί νέους ή αυξημένους κινδύνους κυβερνοασφάλειας, υπό την προϋπόθεση ότι οι παραδοχές και τα μέτρα μετριασμού στα οποία βασίζεται η εκτίμηση κινδύνων παραμένουν έγκυρα και αποτελεσματικά. Ως εκ τούτου, είναι πιθανό η ενημέρωση να μην μπορεί να χαρακτηριστεί ως ουσιαστική τροποποίηση.

112. Αντιθέτως, μια ενημέρωση λογισμικού μπορεί να δημιουργεί νέους φορείς απειλής, να καθιστά δυνατά νέα σενάρια επίθεσης ή να μεταβάλει σε σημαντικό βαθμό την πιθανότητα ή τις επιπτώσεις υφιστάμενων σεναρίων επίθεσης. Στις περιπτώσεις αυτές, ο κατασκευαστής θα πρέπει να επαναξιολογεί τους κινδύνους κυβερνοασφάλειας του προϊόντος με ψηφιακά στοιχεία και να προσδιορίζει αν εξακολουθούν να πληρούνται οι ουσιώδεις απαιτήσεις, συμπεριλαμβανομένου του αν η ενημέρωση δημιουργεί νέους ή αυξημένους κινδύνους που δεν προβλέπονται στην εκτίμηση κινδύνων.

113. Το αν μια ενημέρωση λογισμικού μπορεί να χαρακτηριστεί ως ουσιαστική τροποποίηση είναι σημαντικό για τον προσδιορισμό του αν ισχύουν ορισμένες υποχρεώσεις στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα, όπως ορίζεται στο σημείο 91. Ωστόσο, ανεξάρτητα από τον εν λόγω χαρακτηρισμό, οι κατασκευαστές παραμένουν υπεύθυνοι για τη διασφάλιση της ασφάλειας των ενημερώσεων λογισμικού και του προϊόντος τους με ψηφιακά στοιχεία κατά τη διάρκεια της περιόδου υποστήριξής τους, σύμφωνα με τις απαιτήσεις χειρισμού ευπαθειών που ορίζονται στο παράρτημα I μέρος II του κανονισμού για την κυβερνοανθεκτικότητα. Επιπλέον, ανεξάρτητα από το αν οι ενημερώσεις λογισμικού χαρακτηρίζονται ως ουσιαστικές τροποποιήσεις ή όχι, οι κατασκευαστές υποχρεούνται να διασφαλίζουν ότι η εκτίμηση κινδύνων και ο τεχνικός φάκελος παραμένουν ακριβή, πλήρη και συνεχώς επικαιροποιημένα, σύμφωνα με το άρθρο 13 παράγραφος 7 και το άρθρο 31 παράγραφος 2.

4.4. **Συνέπειες της ουσιαστικής τροποποίησης**

114. Οι συνέπειες της ουσιαστικής τροποποίησης που πραγματοποιείται από φορέα διαφορετικό από τον αρχικό κατασκευαστή προϊόντος με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά εξετάζονται στα άρθρα 21 και 22 του κανονισμού για την κυβερνοανθεκτικότητα. Το άρθρο 21 αφορά τους εισαγωγείς και τους διανομείς, ενώ το άρθρο 22 αφορά κάθε φυσικό ή νομικό πρόσωπο, πέραν του κατασκευαστή, του εισαγωγέα ή του διανομέα.

115. Όταν η ουσιαστική τροποποίηση πραγματοποιείται από τον αρχικό κατασκευαστή του προϊόντος με ψηφιακά στοιχεία, οι συνέπειες απορρέουν από τη γενικά καθιερωμένη έννοια της ουσιαστικής τροποποίησης που αναφέρεται στην αιτιολογική σκέψη 41 του κανονισμού για την κυβερνοανθεκτικότητα και αναλύονται περαιτέρω στο σημείο 2.1 του Γαλάζιου Οδηγού. Στο εν λόγω τμήμα ορίζεται ότι ένα προϊόν που έχει υποστεί σημαντικές αλλαγές ή επισκευές μετά τη θέση του σε κυκλοφορία στην αγορά θεωρείται νέο προϊόν όταν η αρχική επίδοση, ο σκοπός ή ο τύπος του έχουν τροποποιηθεί, η φύση του κινδύνου έχει αλλάξει ή το επίπεδο κινδύνου έχει αυξηθεί και το προϊόν με ψηφιακά στοιχεία διατίθεται στην αγορά.

116. Ως εκ τούτου, η γενικά καθιερωμένη συνέπεια είναι ότι, όταν μια τροποποίηση προϊόντος με ψηφιακά στοιχεία χαρακτηρίζεται ως ουσιαστική τροποποίηση και το τροποποιημένο προϊόν με ψηφιακά στοιχεία διατίθεται στην αγορά, πρέπει να αντιμετωπίζεται ως νέο προϊόν με ψηφιακά στοιχεία για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα. Ως εκ τούτου, η πράξη της διάθεσης του ουσιωδώς τροποποιημένου προϊόντος στην αγορά συνιστά νέα θέση σε κυκλοφορία στην αγορά. Αυτό ισχύει είτε η ουσιαστική τροποποίηση πραγματοποιείται από τον αρχικό κατασκευαστή είτε από άλλο πρόσωπο. Προκειμένου να διασφαλιστεί ότι ο κανονισμός για την κυβερνοανθεκτικότητα εφαρμόζεται με ομοιόμορφο και αναλογικό τρόπο στις διάφορες κατηγορίες φορέων που μπορούν να πραγματοποιήσουν ουσιαστική τροποποίηση, στα ακόλουθα υποτμήματα εξετάζονται οι απορρέουσες υποχρεώσεις του προσώπου που πραγματοποιεί την ουσιαστική τροποποίηση όταν το ουσιωδώς τροποποιημένο προϊόν με ψηφιακά στοιχεία τίθεται σε κυκλοφορία στην αγορά. Οι συνέπειες για την περίοδο υποστήριξης του προϊόντος με ψηφιακά στοιχεία εξετάζονται στο τμήμα *5 Support period*.

4.4.1. *Ουσιαστικές τροποποιήσεις που πραγματοποιούνται από πρόσωπο διαφορετικό από τον αρχικό κατασκευαστή*

117. Σύμφωνα με τα άρθρα 21 και 22, όταν πραγματοποιείται ουσιαστική τροποποίηση προϊόντος με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά από φυσικό ή νομικό πρόσωπο διαφορετικό από τον κατασκευαστή του προϊόντος με ψηφιακά στοιχεία, το πρόσωπο που πραγματοποιεί την ουσιαστική τροποποίηση και διαθέτει το τροποποιημένο προϊόν με ψηφιακά στοιχεία στην αγορά πρέπει να θεωρείται ο κατασκευαστής του τροποποιημένου προϊόντος με ψηφιακά στοιχεία, ανεξάρτητα από το αν το εν λόγω πρόσωπο συμμετείχε στον αρχικό σχεδιασμό ή έθεσε σε κυκλοφορία στην αγορά το εν λόγω προϊόν.

118. Στο άρθρο 22 διευκρινίζεται περαιτέρω ότι το πρόσωπο που πραγματοποιεί την τροποποίηση υπόκειται στις υποχρεώσεις που ορίζονται στα άρθρα 13 και 14 μόνο όσον αφορά το μέρος του προϊόντος με ψηφιακά στοιχεία που επηρεάζεται από την ουσιαστική τροποποίηση, όταν η εν λόγω τροποποίηση δεν έχει επιπτώσεις στην κυβερνοασφάλεια του προϊόντος με ψηφιακά στοιχεία στο σύνολό του.

119. Όταν μια ουσιαστική τροποποίηση επηρεάζει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις, αλλά δεν επηρεάζει αρνητικά την κυβερνοασφάλεια του προϊόντος με ψηφιακά στοιχεία στο σύνολό του, το πρόσωπο που πραγματοποιεί την τροποποίηση υπόκειται στα άρθρα 13 (συμπεριλαμβανομένης της υποχρέωσης να διασφαλίζει τη συμμόρφωση προς τις ουσιώδεις απαιτήσεις και να διενεργεί διαδικασία αξιολόγησης της συμμόρφωσης) και 14 (υποχρεώσεις αναφοράς) μόνο σε σχέση με το μέρος του προϊόντος με ψηφιακά στοιχεία που έχει τροποποιηθεί ουσιωδώς ([16]). Επιπλέον, οι υποχρεώσεις του αρχικού κατασκευαστή σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα εξακολουθούν να ισχύουν για το αρχικό προϊόν με ψηφιακά στοιχεία που τίθεται σε κυκλοφορία στην αγορά, ώστε να διασφαλίζεται η συνέχεια στον χειρισμό ευπαθειών και η συμμόρφωση για τα αμετάβλητα μέρη.

120. Η περίπτωση ουσιαστικής τροποποίησης δεν θα πρέπει να συγχέεται με τις περιπτώσεις ενσωμάτωσης, στις οποίες ένα πρόσωπο συναρμολογεί δομοστοιχεία (μεταξύ άλλων, κατά περίπτωση, τροποποιώντας τα) σε νέο προϊόν με ψηφιακά στοιχεία που το ίδιο θέτει σε κυκλοφορία στην αγορά. Στις περιπτώσεις αυτές, ο συναρμολογητής δεν τροποποιεί προϊόν με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά από άλλον κατασκευαστή· αντιθέτως, θέτει σε κυκλοφορία στην αγορά ένα δικό του νέο προϊόν με ψηφιακά στοιχεία. Ο συναρμολογητής είναι ο κατασκευαστής του εν λόγω νέου προϊόντος με ψηφιακά στοιχεία για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα και υποχρεούται να συμμορφώνεται με τον κανονισμό στο σύνολό του όσον αφορά το προϊόν με ψηφιακά στοιχεία στο σύνολό του. Όταν ο κατασκευαστής ενσωματώνει δομοστοιχεία που υπόκεινται στον κανονισμό για την κυβερνοανθεκτικότητα, μπορεί να βασίζεται στις δραστηριότητες συμμόρφωσης των κατασκευαστών των δομοστοιχείων για να διευκολύνει τη συμμόρφωσή του με τον κανονισμό για την κυβερνοανθεκτικότητα.

Παράδειγμα 51: Εταιρεία αγοράζει έτοιμες προς χρήση μονάδες μικροελεγκτών και δομοστοιχεία συνδεσιμότητας από τρίτους προμηθευτές, αναπτύσσει ιδιόκτητο υλικολογισμικό και πακέτο αισθητήρων και τα συναρμολογεί σε συνδεδεμένο γεωργικό προϊόν παρακολούθησης με ψηφιακά στοιχεία που θέτει σε κυκλοφορία στην αγορά υπό τη δική της επωνυμία. Μολονότι η εταιρεία έχει τροποποιήσει τις υποκείμενες μονάδες μικροελεγκτών και τις έχει συνδυάσει με άλλα δομοστοιχεία, δεν τροποποιεί ουσιωδώς προϊόν με ψηφιακά στοιχεία που έχει ήδη τεθεί σε κυκλοφορία στην αγορά· αντιθέτως, θέτει σε κυκλοφορία στην αγορά νέο προϊόν με ψηφιακά στοιχεία. Η εταιρεία είναι ο κατασκευαστής του γεωργικού συστήματος παρακολούθησης για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα και υποχρεούται να συμμορφώνεται με τον κανονισμό όσον αφορά το γεωργικό σύστημα παρακολούθησης στο σύνολό του.

([16]) Σύμφωνα με το σημείο 2.1 του Γαλάζιου Οδηγού, «[δ]εν είναι απαραίτητο να επαναληφθούν οι δοκιμές και να προσκομιστούν νέα έγγραφα τεκμηρίωσης σε σχέση με πτυχές που δεν επηρεάζονται από την τροποποίηση. Εναπόκειται στο φυσικό ή νομικό πρόσωπο που είτε πραγματοποιεί τις αλλαγές είτε ζητεί να πραγματοποιηθούν αλλαγές στο προϊόν να αποδείξει ότι δεν χρειάζεται να επικαιροποιηθούν όλα τα στοιχεία του τεχνικού φακέλου. Το φυσικό ή νομικό πρόσωπο που πραγματοποιεί τις αλλαγές ή ζητεί να πραγματοποιηθούν αλλαγές στο προϊόν είναι υπεύθυνο για τη συμμόρφωση του τροποποιημένου προϊόντος και συντάσσει δήλωση συμμόρφωσης, ακόμη και αν χρησιμοποιεί υφιστάμενες δοκιμές και τεχνικό φάκελο».

121. Όταν μια ουσιαστική τροποποίηση που πραγματοποιείται από πρόσωπο διαφορετικό από τον αρχικό κατασκευαστή επηρεάζει αρνητικά την κυβερνοασφάλεια του προϊόντος με ψηφιακά στοιχεία στο σύνολό του, για παράδειγμα επειδή η τροποποίηση δεν στοχεύει πλέον ή δεν περιορίζεται σε συγκεκριμένο δομοστοιχείο ή υποσύστημα, το τροποποιημένο προϊόν με ψηφιακά στοιχεία που διατίθεται στην αγορά θα πρέπει να αντιμετωπίζεται ως νέο προϊόν με ψηφιακά στοιχεία που υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα στο σύνολό του. Στις περιπτώσεις αυτές, το συνολικό προφίλ κινδύνου κυβερνοασφάλειας του εν λόγω προϊόντος έχει μεταβληθεί και η τροποποίηση δεν μπορεί να αξιολογηθεί χωρίς να ληφθεί υπόψη το προϊόν με ψηφιακά στοιχεία στο σύνολό του. Το πρόσωπο που πραγματοποιεί την τροποποίηση υπόκειται στις υποχρεώσεις κατασκευαστή που ορίζονται στα άρθρα 13 και 14 όσον αφορά το τροποποιημένο προϊόν με ψηφιακά στοιχεία στο σύνολό του.

4.4.2. *Ουσιαστικές τροποποιήσεις που πραγματοποιούνται από τον αρχικό κατασκευαστή*

122. Όταν η ουσιαστική τροποποίηση πραγματοποιείται από τον αρχικό κατασκευαστή, μεταξύ άλλων στο πλαίσιο της επαναληπτικής ανάπτυξης προϊόντων λογισμικού με ψηφιακά στοιχεία, ο εν λόγω κατασκευαστής παραμένει ο κατασκευαστής για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα. Ωστόσο, το ουσιωδώς τροποποιημένο προϊόν με ψηφιακά στοιχεία πρέπει να θεωρείται ότι τίθεται εκ νέου σε κυκλοφορία στην αγορά.

123. Σύμφωνα με το σημείο 2.1 του Γαλάζιου Οδηγού, ο αρχικός κατασκευαστής που θέτει το ουσιωδώς τροποποιημένο προϊόν με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά μπορεί να επαναχρησιμοποιήσει τα υφιστάμενα έγγραφα τεκμηρίωσης και τις δοκιμές για πτυχές του προϊόντος με ψηφιακά στοιχεία που δεν επηρεάζονται από την ουσιαστική τροποποίηση. Ιδίως όταν ο κατασκευαστής θέτει σε κυκλοφορία στην αγορά ουσιωδώς τροποποιημένες εκδόσεις του ίδιου προϊόντος με ψηφιακά στοιχεία, η διαδικασία αξιολόγησης της συμμόρφωσης θα πρέπει να επικεντρώνεται στα ουσιωδώς τροποποιημένα εξαρτήματα του προϊόντος με ψηφιακά στοιχεία. Ομοίως, όταν διενεργείται αξιολόγηση της συμμόρφωσης από τρίτο, ο οργανισμός αξιολόγησης της συμμόρφωσης θα πρέπει να εστιάζει την αξιολόγησή του στα ουσιωδώς τροποποιημένα εξαρτήματα. Όσον αφορά αμετάβλητα εξαρτήματα του προϊόντος με ψηφιακά στοιχεία, μπορεί να επαναχρησιμοποιήσει τα υφιστάμενα έγγραφα τεκμηρίωσης και τα αποτελέσματα δοκιμών.

124. Οι παράμετροι αναλογικότητας που ορίζονται στο προηγούμενο υποτμήμα ισχύουν εξίσου για τις ουσιαστικές τροποποιήσεις που πραγματοποιούνται από τον αρχικό κατασκευαστή προϊόντος με ψηφιακά στοιχεία που έχει τεθεί σε κυκλοφορία στην αγορά πριν από τις 11 Δεκεμβρίου 2027. Μια τέτοια ουσιαστική τροποποίηση που πραγματοποιείται από τον αρχικό κατασκευαστή δεν απαιτεί, από μόνη της, από τον κατασκευαστή να διασφαλίσει την πλήρη συμμόρφωση ολόκληρου του προϊόντος με ψηφιακά στοιχεία που έχει τεθεί σε κυκλοφορία στην αγορά πριν από την εν λόγω ημερομηνία με τον κανονισμό για την κυβερνοανθεκτικότητα, εκτός εάν η τροποποίηση επηρεάζει αρνητικά την κυβερνοασφάλεια του προϊόντος με ψηφιακά στοιχεία στο σύνολό του. Όταν η τροποποίηση δεν επηρεάζει την κυβερνοασφάλεια του προϊόντος με ψηφιακά στοιχεία στο σύνολό του, οι υποχρεώσεις του αρχικού κατασκευαστή όσον αφορά την τροποποίηση θα πρέπει να περιορίζονται στα ουσιωδώς τροποποιημένα εξαρτήματα.

5. **ΠΕΡΙΟΔΟΣ ΥΠΟΣΤΗΡΙΞΗΣ**

125. Βάσει του άρθρου 13 παράγραφος 8 του κανονισμού για την κυβερνοανθεκτικότητα, οι κατασκευαστές καθορίζουν την περίοδο υποστήριξης κατά την οποία οι ευπάθειες του προϊόντος με ψηφιακά στοιχεία, συμπεριλαμβανομένων των δομοστοιχείων του, αντιμετωπίζονται αποτελεσματικά και σύμφωνα με τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα I μέρος II. Η περίοδος υποστήριξης αντικατοπτρίζει το χρονικό διάστημα κατά το οποίο αναμένεται να χρησιμοποιηθεί το προϊόν με ψηφιακά στοιχεία (τον αναμενόμενο χρόνο χρήσης) και θα πρέπει να καθορίζεται με βάση τα κριτήρια που ορίζονται στο άρθρο 13 παράγραφος 8, ιδίως, τις εύλογες προσδοκίες των χρηστών, τη φύση του προϊόντος με ψηφιακά στοιχεία, συμπεριλαμβανομένου του προβλεπόμενου σκοπού του, καθώς και τη σχετική ενωσιακή νομοθεσία που καθορίζει τη διάρκεια ζωής των προϊόντων με ψηφιακά στοιχεία ([17]). Συνολικά, τα κριτήρια αυτά πρέπει να λαμβάνονται υπόψη με τρόπο που να διασφαλίζει την αναλογικότητα κατά τον καθορισμό της περιόδου υποστήριξης.

([17]) Πρόσθετα κριτήρια που μπορούν να λαμβάνονται υπόψη, σύμφωνα με το άρθρο 13 παράγραφος 8, είναι οι περίοδοι υποστήριξης προϊόντων με ψηφιακά στοιχεία που προσφέρουν παρόμοια λειτουργικότητα και έχουν τεθεί σε κυκλοφορία στην αγορά από άλλους κατασκευαστές, η διαθεσιμότητα του περιβάλλοντος λειτουργίας, οι περίοδοι υποστήριξης των ενσωματωμένων δομοστοιχείων που παρέχουν βασικές λειτουργίες και προέρχονται από τρίτους, καθώς και η σχετική καθοδήγηση που παρέχεται από την ομάδα διοικητικής συνεργασίας (ΕΟΔΚ) του κανονισμού για την κυβερνοανθεκτικότητα και την Επιτροπή.

126. Βάσει του άρθρου 13 παράγραφος 8 απαιτείται επίσης η περίοδος υποστήριξης να είναι τουλάχιστον πέντε έτη, εκτός εάν το προϊόν με ψηφιακά στοιχεία αναμένεται να χρησιμοποιηθεί για λιγότερο από πέντε έτη, οπότε η περίοδος υποστήριξης αντιστοιχεί στον αναμενόμενο χρόνο χρήσης. Ως εκ τούτου, η ελάχιστη περίοδος υποστήριξης λειτουργεί μόνο ως διασφάλιση, εξασφαλίζοντας ότι οι ευπάθειες αντιμετωπίζονται για επαρκώς μεγάλο χρονικό διάστημα και επιτρέποντας παράλληλα στους κατασκευαστές να λαμβάνουν υπόψη προϊόντα με ψηφιακά στοιχεία με πραγματικά συντομότερους αναμενόμενους χρόνους χρήσης. Η αιτιολογική σκέψη 60 παρέχει περισσότερη καθοδήγηση σχετικά με το θέμα αυτό, διευκρινίζοντας ότι τα προϊόντα με ψηφιακά στοιχεία που αναμένεται ευλόγως να χρησιμοποιηθούν για διάστημα μεγαλύτερο των πέντε ετών θα πρέπει, συνεπώς, να έχουν μεγαλύτερες περιόδους υποστήριξης. Ως εκ τούτου, περίοδος υποστήριξης πέντε ετών δεν πρέπει να θεωρείται ο κανόνας για όλα τα προϊόντα με ψηφιακά στοιχεία. Αντ' αυτού, ο κατασκευαστής θα πρέπει να καθορίζει την κατάλληλη περίοδο υποστήριξης με βάση τα κριτήρια που αναφέρονται στο άρθρο 13 παράγραφος 8.

127. Βάσει του άρθρου 13 παράγραφος 19 απαιτείται από τους κατασκευαστές να προσδιορίζεται κατά τη στιγμή της αγοράς, με σαφή και κατανοητό τρόπο, η ημερομηνία λήξης της περιόδου υποστήριξης (τουλάχιστον ο μήνας και το έτος). Απαιτείται επίσης από τους κατασκευαστές να εμφανίζουν κοινοποίηση προς τους χρήστες μετά τη λήξη της περιόδου υποστήριξης, όπου αυτό είναι τεχνικά εφικτό λόγω της φύσης του προϊόντος με ψηφιακά στοιχεία. Η υποχρέωση αυτή αποσκοπεί στην εξασφάλιση διαφάνειας έναντι των χρηστών όσον αφορά το χρονικό διάστημα κατά το οποίο μπορεί να αναμένεται υποστήριξη της ασφάλειας.

128. Στην περίπτωση προϊόντων λογισμικού με ψηφιακά στοιχεία, τα οποία συχνά αναπτύσσονται και διατίθενται στην αγορά με επαναληπτικό τρόπο και σε σχέση με τα οποία συχνά μπορούν να τίθενται σε κυκλοφορία στην αγορά ουσιωδώς τροποποιημένες εκδόσεις σε βάθος χρόνου, η περίοδος υποστήριξης πρέπει να γίνεται αντιληπτή υπό το πρίσμα του συγκεκριμένου μοντέλου ανάπτυξης. Για κάθε ουσιωδώς τροποποιημένη έκδοση προϊόντος λογισμικού με ψηφιακά στοιχεία που τίθεται σε κυκλοφορία στην αγορά πρέπει να υπάρχει δηλωμένη περίοδος υποστήριξης που συμμορφώνεται με το άρθρο 13 παράγραφος 8. Σε αυτήν περιλαμβάνεται η ελάχιστη περίοδος υποστήριξης τουλάχιστον πέντε ετών, εκτός εάν ο αναμενόμενος χρόνος χρήσης της εν λόγω έκδοσης είναι αποδεδειγμένα μικρότερος, όπως διευκρινίζεται επίσης στην αιτιολογική σκέψη 60. Στο τμήμα *5.1 Substantial modifications and the support period* διευκρινίζεται περαιτέρω ότι, όταν η ουσιαστική τροποποίηση δεν οδηγεί σε αλλαγές στους παράγοντες που καθόρισαν αρχικά τον αναμενόμενο χρόνο χρήσης του προϊόντος με ψηφιακά στοιχεία, η αρχική περίοδος υποστήριξης δεν επηρεάζεται (δηλαδή, συμπεριλαμβανομένων των περιπτώσεων στις οποίες η εναπομένουσα περίοδος υποστήριξης είναι μικρότερη από πέντε έτη).

129. Στο άρθρο 13 παράγραφος 10 παρέχεται περιθώριο ευελιξίας για τα προϊόντα λογισμικού με ψηφιακά στοιχεία, καθώς επιτρέπεται στους κατασκευαστές, υπό ορισμένες προϋποθέσεις, να διασφαλίζουν τη συμμόρφωση προς την απαίτηση χειρισμού ευπαθειών που ορίζεται στο παράρτημα I μέρος II σημείο 2 (αντιμετώπιση και διόρθωση ευπαθειών) μόνο για την έκδοση του προϊόντος λογισμικού με ψηφιακά στοιχεία που έθεσαν τελευταία σε κυκλοφορία στην αγορά. Αυτό επιτρέπεται όταν οι χρήστες των εκδόσεων που είχαν τεθεί προηγουμένως σε κυκλοφορία στην αγορά έχουν πρόσβαση στην τελευταία έκδοση που τέθηκε σε κυκλοφορία στην αγορά δωρεάν και δεν επιβαρύνονται με πρόσθετες δαπάνες για την προσαρμογή του περιβάλλοντος υλισμικού και λογισμικού στο οποίο χρησιμοποιούν την αρχική έκδοση του εν λόγω προϊόντος.

130. Για τους σκοπούς του άρθρου 13 παράγραφος 10, η έννοια των «πρόσθετων δαπανών» θα πρέπει να ερμηνεύεται με πρακτικό και αναλογικό τρόπο, λαμβανομένων υπόψη των συνήθων και αναμενόμενων πρακτικών κατά τη συντήρηση και τη λειτουργία του λογισμικού. Δεν περιλαμβάνει εύλογες επιχειρησιακές προσπάθειες που είναι εγγενείς στην εφαρμογή ενημερώσεων λογισμικού ή στη διατήρηση ασφαλούς λειτουργικού περιβάλλοντος, όπως ο χρόνος εργασίας του προσωπικού, οι συνήθεις δοκιμές, οι προσαρμογές διαμόρφωσης ή οι αναβαθμίσεις των υποκείμενων εξαρτήσεων λογισμικού που είναι αναγκαίες για την αντιμετώπιση δομοστοιχείων στο τέλος του κύκλου ζωής τους ή γνωστών ευπαθειών ασφαλείας. Αντιθέτως, οι «πρόσθετες δαπάνες» αφορούν επιβαρύνσεις που υπερβαίνουν τις συνήθως αναμενόμενες δαπάνες στο πλαίσιο των ενημερώσεων λογισμικού, όπως οι υποχρεωτικές αγορές νέου υλισμικού, η αντικατάσταση υποδομών ή οι θεμελιώδεις αλλαγές στο λειτουργικό περιβάλλον.

131. Όσον αφορά συνεχώς εξελισσόμενα προϊόντα λογισμικού με ψηφιακά στοιχεία, οι κατασκευαστές μπορούν να θέτουν σε κυκλοφορία στην αγορά διαδοχικές ουσιωδώς τροποποιημένες εκδόσεις σε σχετικά σύντομα χρονικά διαστήματα και να αναμένουν από τους χρήστες να προβαίνουν σε τακτικές αναβαθμίσεις. Στις περιπτώσεις αυτές, η δηλωθείσα περίοδος υποστήριξης για κάθε ουσιωδώς τροποποιημένη έκδοση πρέπει να συμμορφώνεται με το άρθρο 13 παράγραφος 8 κατά τη στιγμή της θέσης της σε κυκλοφορία στην αγορά. Με άλλα λόγια, ο κατασκευαστής πρέπει να δηλώνει νέα περίοδο υποστήριξης για την εν λόγω ουσιωδώς τροποποιημένη έκδοση. Ωστόσο, οι κατασκευαστές μπορούν να βασίζονται στο άρθρο 13 παράγραφος 10 για να διακόπτουν την αντιμετώπιση και την αποκατάσταση ευπαθειών προγενέστερων

εκδόσεων μόλις οι χρήστες είναι σε θέση να προβούν σε αναβάθμιση σε μεταγενέστερη έκδοση δωρεάν και χωρίς πρόσθετο κόστος, όπως αναφέρεται ανωτέρω, ακόμα και αν αυτό έχει ως αποτέλεσμα μικρότερη πραγματική περίοδο υποστήριξης για τις εν λόγω προγενέστερες εκδόσεις ([18]). Ο κατασκευαστής εξακολουθεί να υπόκειται στις λοιπές απαιτήσεις χειρισμού ευπαθειών του παραρτήματος I μέρος II, καθώς και στις υποχρεώσεις αναφοράς του άρθρου 14. Όπως εξηγείται επίσης στην αιτιολογική σκέψη 40, στις απαιτήσεις αυτές περιλαμβάνονται, μεταξύ άλλων, για όλες τις μεταγενέστερες ουσιωδώς τροποποιημένες εκδόσεις του προϊόντος λογισμικού με ψηφιακά στοιχεία που τίθεται σε κυκλοφορία στην αγορά, τα ακόλουθα: i) διατήρηση πολιτικής για συντονισμένη γνωστοποίηση ευπαθειών· και ii) μέτρα για τη διευκόλυνση της ανταλλαγής πληροφοριών σχετικά με πιθανές ευπάθειες ([19]).

Παράδειγμα 52: Κατασκευαστής θέτει μοντέλο έξυπνου τηλεφώνου σε κυκλοφορία στην αγορά της ΕΕ και δηλώνει περίοδο υποστήριξης Χ ετών από την ημερομηνία θέσης σε κυκλοφορία στην αγορά, κατά τη διάρκεια της οποίας θα παρέχει ενημερώσεις ασφαλείας για την αντιμετώπιση ευπαθειών. Κατά τη διάρκεια αυτής της περιόδου, ο κατασκευαστής διαθέτει στην αγορά τακτικές ενημερώσεις λογισμικού και ουσιωδώς τροποποιημένες εκδόσεις του λειτουργικού συστήματος, τις οποίες οι χρήστες μπορούν να εγκαταστήσουν δωρεάν χωρίς να απαιτείται νέο υλισμικό.

Ο κατασκευαστής μπορεί, σύμφωνα με το άρθρο 13 παράγραφος 10, να αντιμετωπίζει και να διορθώνει τις ευπάθειες της τελευταίας έκδοσης του λειτουργικού συστήματος που διατίθεται για το εν λόγω μοντέλο έξυπνου τηλεφώνου, υπό την προϋπόθεση ότι οι προηγούμενες εκδόσεις μπορούν να αναβαθμιστούν δωρεάν και χωρίς πρόσθετο κόστος. Καθ' όλη τη διάρκεια της περιόδου υποστήριξης, ο κατασκευαστής εξακολουθεί να υπόκειται στις άλλες απαιτήσεις χειρισμού ευπαθειών, όπως η συντονισμένη γνωστοποίηση ευπαθειών και τα μέτρα ανταλλαγής πληροφοριών.

Παράδειγμα 53: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά προϊόν λογισμικού με ψηφιακά στοιχεία για επιχειρήσεις και διαθέτει κάθε λίγους μήνες στην αγορά ουσιωδώς τροποποιημένες εκδόσεις, οι οποίες περιλαμβάνουν βελτιώσεις ασφάλειας, νέα χαρακτηριστικά, και είναι συμβατές με ενημερωμένα λειτουργικά συστήματα και πλατφόρμες. Κάθε έκδοση τίθεται σε κυκλοφορία στην αγορά με δηλωμένη περίοδο υποστήριξης σύμφωνα με το άρθρο 13 παράγραφος 8. Ο κατασκευαστής αναμένει από τους χρήστες να προβαίνουν σε τακτικές αναβαθμίσεις στο πλαίσιο της συνήθους λειτουργίας και παρέχει δωρεάν πρόσβαση στην τελευταία έκδοση. Η εφαρμογή αναβαθμίσεων μπορεί να απαιτεί εύλογη επιχειρησιακή προσπάθεια, όπως δοκιμές ή προσαρμογές διαμόρφωσης, αλλά δεν απαιτεί πρόσθετο κόστος, όπως η αγορά νέου υλισμικού ή θεμελιώδεις αλλαγές υποδομής. Στο πλαίσιο αυτό, ο κατασκευαστής μπορεί να βασίζεται στο άρθρο 13 παράγραφος 10 για να διακόπτει την αντιμετώπιση και την αποκατάσταση ευπαθειών προγενέστερων εκδόσεων μόλις οι χρήστες είναι σε θέση να προβούν σε αναβάθμιση στην τελευταία έκδοση, εξακολουθώντας, παράλληλα, να συμμορφώνεται προς τις λοιπές απαιτήσεις χειρισμού ευπαθειών για όλες τις μεταγενέστερες ουσιωδώς τροποποιημένες εκδόσεις.

5.1. **Ουσιαστικές τροποποιήσεις και η περίοδος υποστήριξης**

132. Όπως ορίζεται στο τμήμα *4.4 Consequences of a substantial modification,* όταν μια τροποποίηση προϊόντος με ψηφιακά στοιχεία χαρακτηρίζεται ως ουσιαστική τροποποίηση και το τροποποιημένο προϊόν με ψηφιακά στοιχεία διατίθεται στην αγορά, πρέπει να αντιμετωπίζεται ως νέο προϊόν για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα, και η πράξη της διάθεσης του ουσιωδώς τροποποιημένου προϊόντος με ψηφιακά στοιχεία στην αγορά αποτελεί νέα θέση σε κυκλοφορία στην αγορά. Ως εκ τούτου, είναι χρήσιμο να διευκρινιστεί η επίδραση που έχει η εν λόγω νέα θέση σε κυκλοφορία στην αγορά στην περίοδο υποστήριξης του ουσιωδώς τροποποιημένου προϊόντος με ψηφιακά στοιχεία.

133. Η περίοδος υποστήριξης ουσιωδώς τροποποιημένου προϊόντος με ψηφιακά στοιχεία θα πρέπει να καθορίζεται με βάση τον αναμενόμενο χρόνο χρήσης του εν λόγω προϊόντος, υπό το πρίσμα των κριτηρίων που ορίζονται στο άρθρο 13 παράγραφος 8 του κανονισμού για την κυβερνοανθεκτικότητα. Ως εκ τούτου, η ύπαρξη ουσιαστικής τροποποίησης θα πρέπει να συνεπάγεται επαναξιολόγηση με βάση τα εν λόγω κριτήρια, αλλά δεν έχει αυτομάτως ως αποτέλεσμα τον επανακαθορισμό ή ακόμα και την παράταση της περιόδου υποστήριξης. Το κρίσιμο ζήτημα είναι αν η ουσιαστική τροποποίηση επηρεάζει τους παράγοντες βάσει των οποίων είχε καθοριστεί αρχικά ο αναμενόμενος χρόνος χρήσης του εν λόγω προϊόντος και, ως εκ τούτου, η αρχική περίοδος υποστήριξης.

([18]) Υπενθυμίζεται ότι βάσει του άρθρου 13 παράγραφος 19 απαιτείται από τους κατασκευαστές, όπου είναι τεχνικά εφικτό λόγω της φύσης του προϊόντος με ψηφιακά στοιχεία, να εμφανίζουν κοινοποίηση προς τους χρήστες με την οποία τους ενημερώνουν ότι το προϊόν τους με ψηφιακά στοιχεία έχει φτάσει στο τέλος της περιόδου υποστήριξής του. Ως εκ τούτου, όταν διακόπτεται η αντιμετώπιση και η διόρθωση ευπαθειών προγενέστερων εκδόσεων, αναμένεται ότι οι χρήστες που δεν έχουν προβεί σε αναβάθμιση στην πλέον πρόσφατη έκδοση θα ενημερώνονται, εάν αυτό είναι τεχνικά εφικτό.

([19]) Θα πρέπει να σημειωθεί ότι, όταν οι χρήστες μπορούν να προβούν σε αναβάθμιση στην τελευταία έκδοση του λογισμικού χωρίς πρόσθετο κόστος, οι κατασκευαστές μπορούν, ωστόσο, να επιλέξουν να συνεχίσουν να αντιμετωπίζουν και να διορθώνουν τις ευπάθειες σε προγενέστερες εκδόσεις του εν λόγω λογισμικού, μεταξύ άλλων επί πληρωμή ή βάσει άλλων εμπορικών ρυθμίσεων. Ο κανονισμός για την κυβερνοανθεκτικότητα δεν υποχρεώνει τους κατασκευαστές να παρέχουν δωρεάν ενημερώσεις ασφαλείας για τις εν λόγω προγενέστερες εκδόσεις.

134. Όταν η ουσιαστική τροποποίηση δεν επηρεάζει τους εν λόγω παράγοντες, τα κριτήρια που ορίζονται στο άρθρο 13 παράγραφος 8 εξακολουθούν να συνεπάγονται τον ίδιο αναμενόμενο χρόνο χρήσης όπως είχε αρχικά καθοριστεί και η περίοδος υποστήριξης του τροποποιημένου προϊόντος με ψηφιακά στοιχεία θα πρέπει να ευθυγραμμίζεται με τον εναπομένοντα αναμενόμενο χρόνο χρήσης του προϊόντος όπως τέθηκε αρχικά σε κυκλοφορία στην αγορά. Αυτό συμβαίνει συνήθως όταν ο αναμενόμενος χρόνος χρήσης καθορίστηκε κυρίως με βάση παράγοντες τους οποίους δεν μεταβάλλει η τροποποίηση, όπως η φυσική ανθεκτικότητα των δομοστοιχείων υλισμικού, όταν η ουσιαστική τροποποίηση αφορά μόνο τη λειτουργικότητα του λογισμικού ή υπηρεσίες υποστηρικτικών λειτουργιών.

Παράδειγμα 54: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά ρομποτική ηλεκτρική σκούπα με αναμενόμενο χρόνο χρήσης Χ ετών, ο οποίος καθορίζεται με βάση τη φύση του προϊόντος με ψηφιακά στοιχεία, συμπεριλαμβανομένης της φυσικής ανθεκτικότητας και των χαρακτηριστικών αντοχής στη φθορά των δομοστοιχείων υλισμικού και λαμβανομένων υπόψη των εύλογων προσδοκιών των χρηστών όσον αφορά τη διάρκεια ζωής του εν λόγω προϊόντος. Ο κατασκευαστής ορίζει περίοδο υποστήριξης Χ ετών. Μετά από Υ έτη, ο κατασκευαστής διαθέτει ενημέρωση λογισμικού που χαρακτηρίζεται ως ουσιαστική τροποποίηση, προσθέτοντας νέους τρόπους καθαρισμού και χαρακτηριστικά πλοήγησης. Η ενημέρωση λογισμικού δεν επηρεάζει τη φυσική ανθεκτικότητα του υλισμικού και δεν μεταβάλλει τις εύλογες προσδοκίες των χρηστών όσον αφορά τη διάρκεια ζωής του εν λόγω προϊόντος. Ως εκ τούτου, τα κριτήρια του άρθρου 13 παράγραφος 8 εξακολουθούν να συνεπάγονται τον ίδιο αναμενόμενο χρόνο χρήσης. Η περίοδος υποστήριξης του τροποποιημένου προϊόντος με ψηφιακά στοιχεία ευθυγραμμίζεται με τον εναπομένοντα αναμενόμενο χρόνο χρήσης, όπως καθορίστηκε αρχικά.

Παράδειγμα 55: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά σύνθετο βιομηχανικό μηχανολογικό προϊόν με ψηφιακά στοιχεία, με σύστημα υποστηρικτικών λειτουργιών υπολογιστικού νέφους που αποτελεί λύση εξ αποστάσεως επεξεργασίας δεδομένων. Ο αναμενόμενος χρόνος χρήσης είναι Χ έτη και καθορίζεται με βάση τις εύλογες προσδοκίες των χρηστών και τη φύση του προϊόντος με ψηφιακά στοιχεία, όπως η φυσική ανθεκτικότητα του υλισμικού του μηχανήματος και η αναμενόμενη φθορά. Η περίοδος υποστήριξης ορίζεται έτσι ώστε να ευθυγραμμίζεται με τον εν λόγω αναμενόμενο χρόνο χρήσης στα Χ έτη. Μετά από Υ έτη, ο κατασκευαστής αναδιαμορφώνει το σύστημα υποστηρικτικών λειτουργιών υπολογιστικού νέφους (λύση εξ αποστάσεως επεξεργασίας δεδομένων), εισάγοντας νέα API και ροές δεδομένων, με τρόπο που μπορεί να χαρακτηριστεί ως ουσιαστική τροποποίηση του προϊόντος με ψηφιακά στοιχεία, αλλά δεν μεταβάλλει τη φύση του εν λόγω προϊόντος ούτε επηρεάζει τις προσδοκίες των χρηστών. Ως εκ τούτου, τα κριτήρια του άρθρου 13 παράγραφος 8 εξακολουθούν να συνεπάγονται τον ίδιο αναμενόμενο χρόνο χρήσης. Η περίοδος υποστήριξης του τροποποιημένου προϊόντος με ψηφιακά στοιχεία ευθυγραμμίζεται με τον εναπομένοντα αναμενόμενο χρόνο χρήσης, όπως καθορίστηκε αρχικά.

135. Όταν η ουσιαστική τροποποίηση επηρεάζει τους παράγοντες που είχαν καθορίσει αρχικά τον αναμενόμενο χρόνο χρήσης του προϊόντος με ψηφιακά στοιχεία, ο κατασκευαστής θα πρέπει να υπολογίζει εκ νέου την περίοδο υποστήριξης ώστε να αντικατοπτρίζει τον νέο αναμενόμενο χρόνο χρήσης, εφαρμόζοντας αναλόγως τα κριτήρια του άρθρου 13 παράγραφος 8. Αυτό μπορεί να συμβαίνει, για παράδειγμα, στην περίπτωση τροποποιήσεων του υλισμικού που παρατείνουν τη λειτουργική διάρκεια ζωής του εν λόγω προϊόντος ή ουσιώδους αναπρογραμματισμού ή επανασυγγραφής του βασικού λογισμικού του εν λόγω προϊόντος που μεταβάλλει ουσιωδώς τον αναμενόμενο χρόνο χρήσης του ([20]).

Παράδειγμα 56: Κατασκευαστής θέτει σε κυκλοφορία στην αγορά προγραμματιζόμενο λογικό ελεγκτή (PLC) με αναμενόμενο χρόνο χρήσης Χ ετών, ο οποίος καθορίζεται κυρίως με βάση τη φύση του προϊόντος με ψηφιακά στοιχεία και την ανθεκτικότητα του υποκείμενου υλισμικού. Η περίοδος υποστήριξης ορίζεται αναλόγως. Αρκετά έτη μετά την αρχική θέση σε κυκλοφορία στην αγορά, ο κατασκευαστής προβαίνει σε ουσιαστική τροποποίηση που συνίσταται στην αντικατάσταση της ενσωματωμένης υπολογιστικής πλατφόρμας του PLC, συμπεριλαμβανομένου του επεξεργαστή, της μνήμης και του περιβάλλοντος εκτέλεσης, με μια νέα γενιά δομοστοιχείων σχεδιασμένων για σημαντικά μεγαλύτερη λειτουργική διάρκεια ζωής. Ως αποτέλεσμα της τροποποίησης, οι εύλογες προσδοκίες των χρηστών και η φύση του προϊόντος με ψηφιακά στοιχεία μεταβάλλονται: ο χρήστης του PLC μπορεί πλέον εύλογα να αναμένει ότι το PLC θα παραμείνει σε παραγωγική χρήση πέραν του αρχικά δηλωθέντος αναμενόμενου χρόνου χρήσης του, καθώς θα υποστηρίζεται από τη νέα υπολογιστική πλατφόρμα. Ως εκ τούτου, τα κριτήρια του άρθρου 13 παράγραφος 8 συνεπάγονται μεγαλύτερο αναμενόμενο χρόνο χρήσης και ο κατασκευαστής υπολογίζει εκ νέου την περίοδο υποστήριξης για το συγκεκριμένο PLC αναλόγως.

6. **ΣΗΜΑΝΤΙΚΑ ΚΑΙ ΚΡΙΣΙΜΑ ΠΡΟΪΟΝΤΑ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ**

136. Το άρθρο 7 παράγραφος 1 του κανονισμού για την κυβερνοανθεκτικότητα ορίζει ότι τα προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργικότητα μιας κατηγορίας προϊόντων που ορίζεται στο παράρτημα ΙΙΙ του κανονισμού θεωρούνται «σημαντικά προϊόντα με ψηφιακά στοιχεία». Το παράρτημα ΙΙΙ διαιρεί περαιτέρω τα σημαντικά προϊόντα με ψηφιακά στοιχεία στις κλάσεις Ι και ΙΙ. Ομοίως, το άρθρο 8 παράγραφος 1 ορίζει ότι τα προϊόντα με ψηφιακά στοιχεία που έχουν τη βασική λειτουργικότητα μιας κατηγορίας προϊόντων που ορίζεται στο παράρτημα IV του κανονισμού για την κυβερνοανθεκτικότητα θεωρούνται «κρίσιμα προϊόντα με ψηφιακά στοιχεία» ([21]).

([20]) Υπενθυμίζεται ότι, όπως αναφέρεται στο τμήμα *4.1 Physical repairs*, οι εργασίες ανακατασκευής, συντήρησης ή επισκευής δεν θεωρείται γενικά ότι ισοδυναμούν με ουσιαστικές τροποποιήσεις.

([21]) Ο εκτελεστικός κανονισμός (ΕΕ) 2025/2392 της Επιτροπής καθορίζει την τεχνική περιγραφή των κατηγοριών σημαντικών και κρίσιμων προϊόντων.

137. Η ταξινόμηση ενός προϊόντος με ψηφιακά στοιχεία ως σημαντικού ή κρίσιμου ή, αντιθέτως, ως προϊόντος που ανήκει στην κατηγορία «κανονικών» προϊόντων ([22]), είναι σημαντική κατά τον προσδιορισμό της διαδικασίας αξιολόγησης της συμμόρφωσης που πρέπει να ακολουθήσει ο κατασκευαστής, σύμφωνα με το άρθρο 32, ώστε να μπορέσει να θέσει σε κυκλοφορία στην αγορά το εν λόγω προϊόν με ψηφιακά στοιχεία. Ειδικότερα, τα προϊόντα με ψηφιακά στοιχεία στην κατηγορία «κανονικών» προϊόντων μπορούν πάντα να βασίζονται στη διαδικασία εσωτερικού ελέγχου βάσει της ενότητας Α («αυτοαξιολόγηση») ([23]). Τα σημαντικά προϊόντα με ψηφιακά στοιχεία της κλάσης Ι ή ΙΙ και τα κρίσιμα προϊόντα με ψηφιακά στοιχεία υπόκεινται σε αυστηρότερες διαδικασίες αξιολόγησης της συμμόρφωσης. Δεν περιλαμβάνονται τα σημαντικά προϊόντα με ψηφιακά στοιχεία της κλάσης Ι ή ΙΙ που χαρακτηρίζονται ως ελεύθερο λογισμικό ανοικτού κώδικα και τίθενται σε κυκλοφορία στην αγορά, για τα οποία, σύμφωνα με το άρθρο 32 παράγραφος 5, οι κατασκευαστές επιτρέπεται να ακολουθούν τις διαδικασίες της κατηγορίας «κανονικών» προϊόντων.

138. Ως εκ τούτου, η έννοια της βασικής λειτουργικότητας είναι απαραίτητη προκειμένου ο κατασκευαστής να καθορίσει το εφαρμοστέο καθεστώς αξιολόγησης της συμμόρφωσης. Ωστόσο, η έννοια αυτή δεν ορίζεται ρητά στον κανονισμό για την κυβερνοανθεκτικότητα. Τα προϊόντα με ψηφιακά στοιχεία μπορούν να εκτελούν διάφορες λειτουργίες, ορισμένες από τις οποίες μπορεί να είναι βοηθητικές της βασικής λειτουργικότητας του εν λόγω προϊόντος και δεν θα πρέπει να επηρεάζουν την ταξινόμηση του προϊόντος ως «κανονικού»/σημαντικού κλάσης Ι/σημαντικού κλάσης ΙΙ/κρίσιμου. Ως εκ τούτου, είναι χρήσιμο να παρασχεθεί περαιτέρω καθοδήγηση ώστε να βοηθηθούν οι κατασκευαστές να εκτελούν ορθά τις σχετικές διαδικασίες αξιολόγησης της συμμόρφωσης και να βοηθηθούν οι αρχές εποπτείας της αγοράς να διασφαλίζουν την εναρμονισμένη επιβολή του κανονισμού για την κυβερνοανθεκτικότητα σε ολόκληρη την ΕΕ.

6.1. **Βασική λειτουργικότητα**

139. Η βασική λειτουργικότητα ενός προϊόντος με ψηφιακά στοιχεία αναφέρεται στα κύρια χαρακτηριστικά και στις τεχνικές ικανότητες του εν λόγω προϊόντος, χωρίς τα οποία δεν θα ήταν σε θέση να εκπληρώσει τον επιδιωκόμενο σκοπό του. Μπορεί να αξιολογηθεί υπό το πρίσμα του ειδικού πλαισίου και των όρων χρήσης του εν λόγω προϊόντος, λαμβανομένων υπόψη, μεταξύ άλλων, των πληροφοριών που παρέχει ο κατασκευαστής στις οδηγίες χρήσης, σε διαφημιστικό υλικό ή στο υλικό πωλήσεων και σε δηλώσεις, καθώς και στον τεχνικό φάκελο.

Παράδειγμα 57: Προϊόν λογισμικού με ψηφιακά στοιχεία παρέχει ένα επίπεδο αφαίρεσης πάνω από το υποκείμενο υλισμικό και διαχειρίζεται την εκτέλεση δομοστοιχείων λογισμικού. Στα κύρια χαρακτηριστικά του περιλαμβάνονται η αρχικοποίηση υλισμικού και περιφερειακών, η διαχείριση διεργασιών και μνήμης, ο έλεγχος εισροών-εκροών, ο προγραμματισμός, η κατανομή πόρων και η έκθεση υπηρεσιών συστήματος και διεπαφών προγραμματισμού εφαρμογών (API) μέσω των οποίων οι εφαρμογές αλληλεπιδρούν με πόρους του υλισμικού και λογισμικού της συσκευής. Στον τεχνικό φάκελο αναφέρεται ότι το προϊόν με ψηφιακά στοιχεία ενορχηστρώνει τους υπολογιστικούς πόρους, επιβάλλει διαμορφώσεις συστήματος και παρέχει τυποποιημένες διεπαφές για ενότητες λογισμικού και συνδεδεμένα περιφερειακά. Ο κατασκευαστής επισημαίνει ότι οι ικανότητες αυτές επιτρέπουν στην πλατφόρμα να λειτουργεί ως το κεντρικό περιβάλλον λογισμικού στο οποίο μπορούν να λειτουργούν αξιόπιστα οι εφαρμογές. Το προϊόν με ψηφιακά στοιχεία έχει τη βασική λειτουργικότητα λειτουργικού συστήματος, όπως περιγράφεται στο παράρτημα Ι σημείο 11 του εκτελεστικού κανονισμού (ΕΕ) 2025/2392.

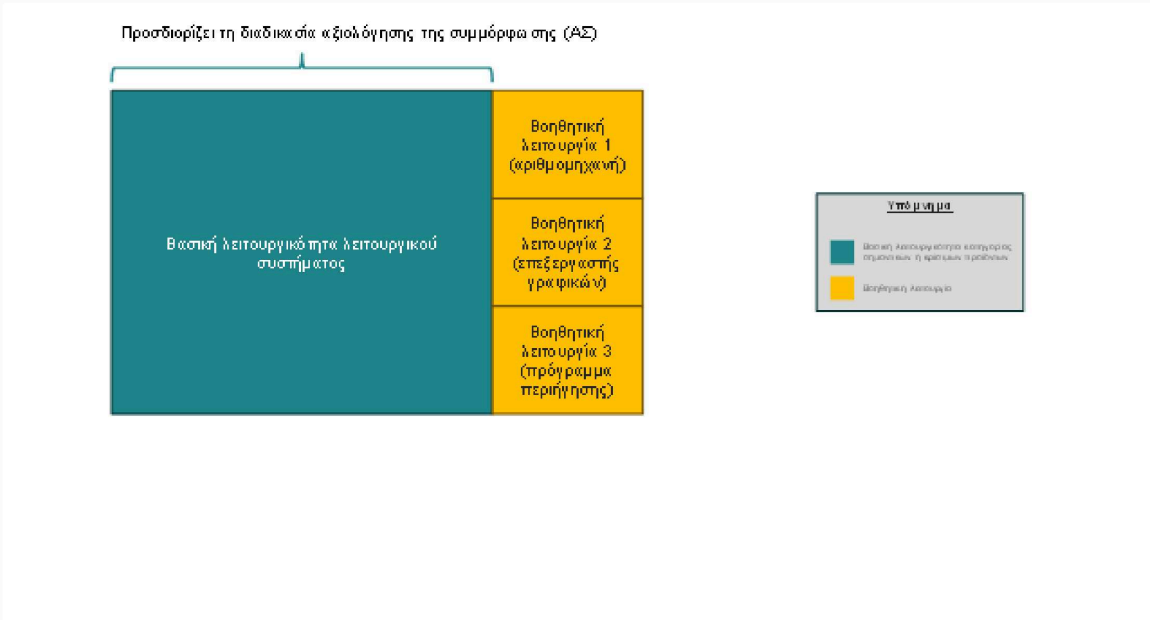
140. Η λειτουργικότητα ενός προϊόντος με ψηφιακά στοιχεία σπανίως περιορίζεται αποκλειστικά στη βασική λειτουργικότητά του, καθώς τα προϊόντα με ψηφιακά στοιχεία συχνά, αν όχι πάντα, εκτελούν πρόσθετες λειτουργίες που δεν συμβάλλουν στη βασική λειτουργικότητα του προϊόντος. Σε αυτό το πλαίσιο, μπορεί επίσης να περιλαμβάνεται η ενσωμάτωση δομοστοιχείων που έχουν τα ίδια τη λειτουργικότητα άλλου σημαντικού ή κρίσιμου προϊόντος με ψηφιακά στοιχεία. Ωστόσο, το γεγονός ότι ένα προϊόν με ψηφιακά στοιχεία εκτελεί λειτουργίες διαφορετικές ή επιπρόσθετες εκείνων που περιγράφονται λεπτομερώς στις τεχνικές περιγραφές σημαντικών ή κρίσιμων προϊόντων με ψηφιακά στοιχεία δεν εμποδίζει αφ' εαυτού το προϊόν να έχει μία τέτοια βασική λειτουργικότητα.

([22]) Ο όρος κατηγορία «κανονικών» προϊόντων δεν αποτελεί όρο που ορίζεται στον κανονισμό για την κυβερνοανθεκτικότητα. Η χρήση του όρου στο παρόν έγγραφο αφορά προϊόντα με ψηφιακά στοιχεία που δεν έχουν τη βασική λειτουργικότητα κατηγορίας προϊόντων που ορίζεται στα παραρτήματα ΙΙΙ ή IV του κανονισμού για την κυβερνοανθεκτικότητα και τα οποία, κατά συνέπεια, υπόκεινται στο καθεστώς αξιολόγησης της συμμόρφωσης που ορίζεται στο άρθρο 32 παράγραφος 1.

([23]) Ωστόσο, ο κατασκευαστής μπορεί πάντα να επιλέξει να εφαρμόσει αυστηρότερη διαδικασία αξιολόγησης της συμμόρφωσης, όπως ορίζεται στο άρθρο 32 παράγραφος 1.

Διάγραμμα 2

Απεικόνιση του τρόπου με τον οποίο η βασική λειτουργικότητα και όχι οι βοηθητικές λειτουργίες καθορίζουν την εφαρμοστέα διαδικασία αξιολόγησης της συμμόρφωσης



141. Ένα προϊόν με ψηφιακά στοιχεία μπορεί να έχει την ικανότητα να εκτελεί τις λειτουργίες μιας σημαντικής ή κρίσιμης κατηγορίας προϊόντων και, παρά ταύτα, να έχει βασική λειτουργικότητα διαφορετική από εκείνη μιας τέτοιας κατηγορίας προϊόντων. Στις περιπτώσεις αυτές, το εν λόγω προϊόν με ψηφιακά στοιχεία δεν μπορεί να χαρακτηριστεί ως σημαντικό ή κρίσιμο προϊόν με ψηφιακά στοιχεία. Όπως αναφέρεται ρητά στο άρθρο 7 παράγραφος 1 του κανονισμού για την κυβερνοανθεκτικότητα σχετικά με τα σημαντικά προϊόντα με ψηφιακά στοιχεία (και εφαρμόζοντας την ίδια λογική για τα κρίσιμα προϊόντα με ψηφιακά στοιχεία), η ενσωμάτωση ενός σημαντικού ή κρίσιμου προϊόντος με ψηφιακά στοιχεία δεν καθιστά από μόνη της το προϊόν με ψηφιακά στοιχεία σημαντικό ή κρίσιμο προϊόν με ψηφιακά στοιχεία.

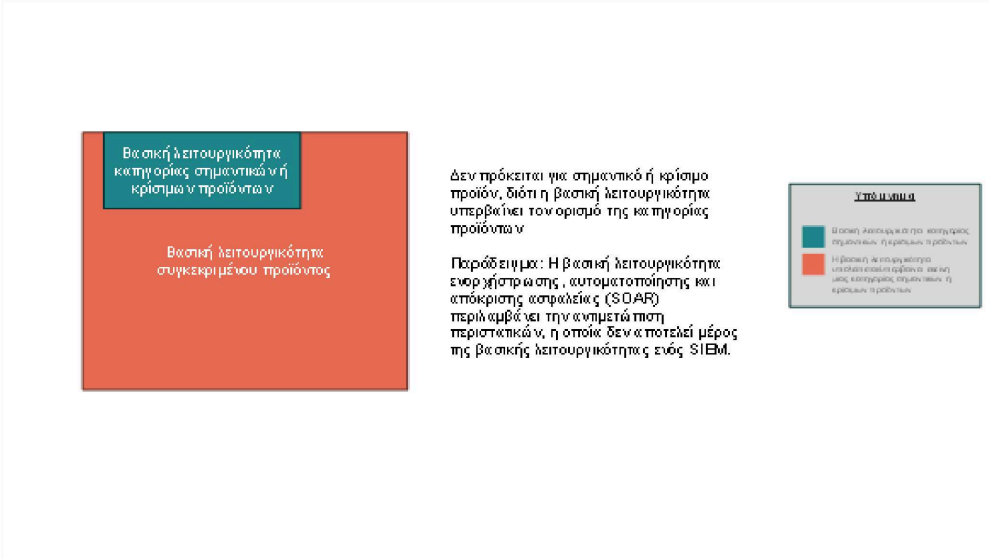
Παράδειγμα 58: Ένα έξυπνο τηλέφωνο ενσωματώνει λειτουργικό σύστημα που παρέχει τις λειτουργίες που περιγράφονται στο παράρτημα I σημείο 11 του εκτελεστικού κανονισμού (ΕΕ) 2025/2392. Ενώ το λειτουργικό σύστημα επιτρέπει τη διαχείριση πόρων υλισμικού και την εκτέλεση εφαρμογών λογισμικού, το έξυπνο τηλέφωνο στο σύνολό του έχει διαφορετική βασική λειτουργικότητα (π.χ. εκείνη της παροχής στους χρήστες της δυνατότητας να επικοινωνούν και να έχουν πρόσβαση σε πληροφορίες και υπηρεσίες). Η ενσωμάτωση ενός λειτουργικού συστήματος δεν συνεπάγεται από μόνη της ότι το έξυπνο τηλέφωνο έχει τη βασική λειτουργικότητα ενός λειτουργικού συστήματος.

142. Ορισμένα προϊόντα με ψηφιακά στοιχεία μπορεί να είναι παρόμοια με κατηγορία σημαντικών ή κρίσιμων προϊόντων ή μπορεί να ανήκουν στην ίδια γενική οικογένεια προϊόντων, ωστόσο η βασική λειτουργικότητά τους ενδέχεται να υπερβαίνει ουσιωδώς ή να υπολείπεται ουσιωδώς της βασικής λειτουργικότητας της εν λόγω κατηγορίας. Αυτό δεν ισχύει όταν ένα προϊόν με ψηφιακά στοιχεία περιλαμβάνει πρόσθετες λειτουργικότητες που απλώς συμπληρώνουν ή ενισχύουν τη βασική λειτουργικότητα, η οποία με τη σειρά της αντιστοιχεί σε εκείνη κατηγορίας σημαντικών ή κρίσιμων προϊόντων· στις περιπτώσεις αυτές, το προϊόν με ψηφιακά στοιχεία διατηρεί τη βασική λειτουργικότητα της εν λόγω κατηγορίας και ταξινομείται αναλόγως. Η αξιολόγηση αυτή θα πρέπει να βασίζεται στα κύρια χαρακτηριστικά και στις τεχνικές ικανότητες του εν λόγω προϊόντος, εξεταζόμενα αντικειμενικά υπό το πρίσμα του επιδιωκόμενου σκοπού του, και όχι στον τρόπο με τον οποίο περιγράφεται ή διατίθεται στην αγορά το προϊόν με ψηφιακά στοιχεία, όταν η εν λόγω περιγραφή δεν αντικατοπτρίζει τα πραγματικά τεχνικά χαρακτηριστικά του προϊόντος.

Παράδειγμα 59: Ένα λογισμικό ενορχήστρωσης, αυτοματοποίησης και απόκρισης ασφαλείας (SOAR) έχει συχνά την ικανότητα να εκτελεί τις λειτουργίες προϊόντων με ψηφιακά στοιχεία στην κατηγορία των «συστημάτων διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM)», δηλαδή να συλλέγει δεδομένα από πολλαπλές πηγές, να τα αναλύει, να τα συσχετίζει και να τα παρουσιάζει ως αξιοποιήσιμες πληροφορίες για σκοπούς που σχετίζονται με την ασφάλεια. Ωστόσο, η βασική λειτουργικότητα του λογισμικού υπερβαίνει ουσιωδώς τη βασική λειτουργικότητα ενός SIEM, καθώς περιλαμβάνει υπηρεσίες όπως η αντιμετώπιση περιστατικών ως βασικά στοιχεία των τεχνικών ικανοτήτων του. Ως εκ τούτου, το λογισμικό SOAR γενικά δεν θεωρείται ότι έχει τη βασική λειτουργικότητα των συστημάτων SIEM.

Διάγραμμα 3

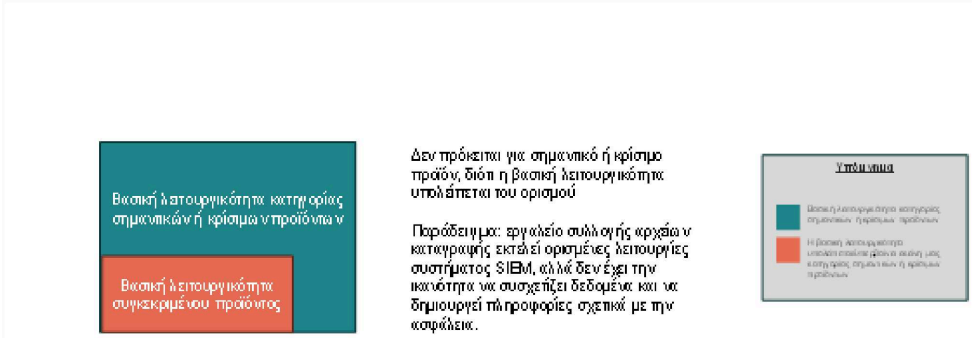
Απεικόνιση της βασικής λειτουργικότητας προϊόντος με ψηφιακά στοιχεία που υπερβαίνουν ουσιωδώς τον ορισμό κατηγορίας σημαντικών ή κρίσιμων προϊόντων



Παράδειγμα 60: Ορισμένα εργαλεία συλλογής και απεικόνισης αρχείων καταγραφής έχουν την ικανότητα να λαμβάνουν δεδομένα αρχείων καταγραφής και να παρουσιάζουν βασικούς πίνακες που απεικονίζουν συμβάντα του συστήματος. Παρότι τα εργαλεία αυτά μπορούν να υποστηρίξουν δραστηριότητες παρακολούθησης της ασφάλειας, η βασική λειτουργικότητά τους υπολείπεται εκείνης των συστημάτων SIEM, καθώς δεν εκτελούν συσχέτιση δεδομένων ούτε παρέχουν αξιοποιήσιμες πληροφορίες ασφάλειας. Ως εκ τούτου, τα εργαλεία αυτά δεν πρέπει γενικά να θεωρείται ότι έχουν τη βασική λειτουργικότητα των συστημάτων SIEM.

Διάγραμμα 4

Απεικόνιση της βασικής λειτουργικότητας προϊόντος με ψηφιακά στοιχεία που υπολείπεται σημαντικά του ορισμού κατηγορίας σημαντικών ή κρίσιμων προϊόντων

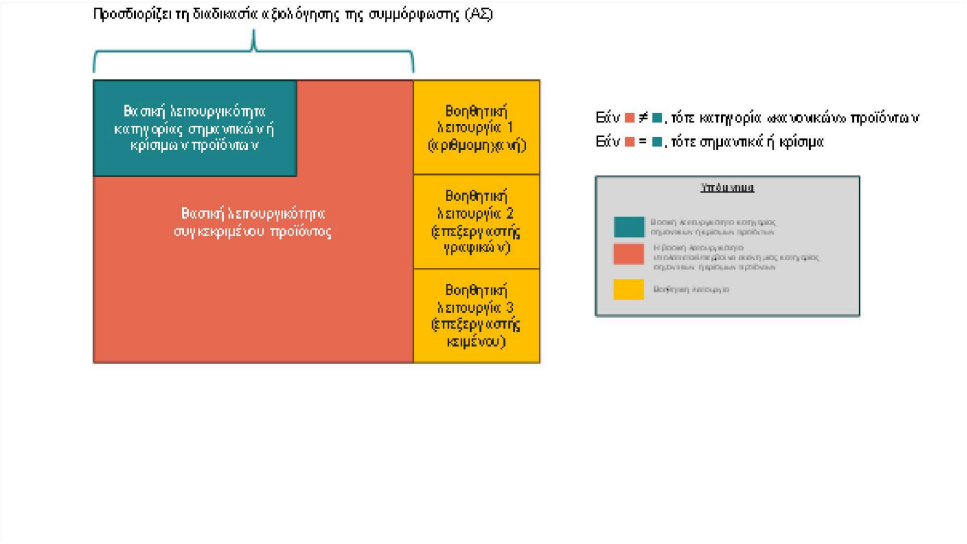


143. Ένας κατασκευαστής δεν μπορεί να παρουσιάζει με παραπλανητικό τρόπο τη βασική λειτουργικότητα του προϊόντος του με ψηφιακά στοιχεία ώστε να αποφεύγει το καθεστώς αξιολόγησης της συμμόρφωσης που εφαρμόζεται σε σημαντικά ή κρίσιμα προϊόντα με ψηφιακά στοιχεία, π.χ. δίνοντας υπερβολική έμφαση ή υποβαθμίζοντας τον ρόλο ορισμένων λειτουργιών, έτσι ώστε το προϊόν να υπερβαίνει ή να υπολείπεται ουσιωδώς μιας δεδομένης βασικής λειτουργικότητας. Αυτό συμβαίνει, για παράδειγμα, όταν υπάρχουν σαφείς ασυνέπειες μεταξύ του διαφημιστικού υλικού, των οδηγιών χρήσης και του τεχνικού φακέλου.

144. Ένα προϊόν με ψηφιακά στοιχεία δεν μπορεί να έχει περισσότερες από μία βασικές λειτουργικότητες για τους σκοπούς του καθορισμού του εφαρμοστέου καθεστώτος αξιολόγησης της συμμόρφωσης. Σύμφωνα με το παράρτημα VII του κανονισμού για την κυβερνοανθεκτικότητα, στο πλαίσιο του τεχνικού φακέλου ενός προϊόντος, οι κατασκευαστές υποχρεούνται να περιγράφουν τον επιδιωκόμενο σκοπό του προϊόντος τους με ψηφιακά στοιχεία και τη διαδικασία αξιολόγησης της συμμόρφωσης που έχουν εφαρμόσει. Ως εκ τούτου, η βασική λειτουργικότητα του προϊόντος θα πρέπει να προσδιορίζεται σαφώς. Με αυτόν τον τρόπο καθίσταται δυνατός ο ορθός προσδιορισμός του εφαρμοστέου καθεστώτος αξιολόγησης της συμμόρφωσης και παρέχεται στις αρχές εποπτείας της αγοράς η δυνατότητα να εποπτεύουν και να ελέγχουν την ορθή εφαρμογή του κανονισμού.

Διάγραμμα 5

Απεικόνιση του τρόπου με τον οποίο η βασική λειτουργικότητα συγκεκριμένου προϊόντος με ψηφιακά στοιχεία καθορίζει την κλάση προϊόντος και, ως εκ τούτου, την εφαρμοστέα διαδικασία αξιολόγησης της συμμόρφωσης



145. Ορισμένα προϊόντα με ψηφιακά στοιχεία τίθενται σε κυκλοφορία στην αγορά ως ενιαία προϊόντα με ψηφιακά στοιχεία, αλλά αποτελούνται από διακριτές μονάδες με χωριστές λειτουργίες. Όταν ένας κατασκευαστής διαθέτει επίσης τις εν λόγω μονάδες στην αγορά χωριστά, όπως στην περίπτωση που αυτές προσφέρονται χωριστά για αγορά, αδειοδότηση ή συνδρομή, οι εν λόγω μονάδες αποτελούν αυτόνομα προϊόντα με ψηφιακά στοιχεία. Επομένως, πρέπει να ταξινομούνται με βάση τις αντίστοιχες βασικές λειτουργικότητές τους (και, ως εκ τούτου, να υπόκεινται στο κατάλληλο καθεστώς αξιολόγησης της συμμόρφωσης με βάση τη βασική λειτουργικότητα κάθε μονάδας). Αυτό ισχύει με την επιφύλαξη των μονάδων που παρέχονται αποκλειστικά ως δομοστοιχεία ολοκληρωμένου προϊόντος με ψηφιακά στοιχεία και δεν διατίθενται χωριστά· στις περιπτώσεις αυτές, η βασική λειτουργικότητα καθορίζεται στο επίπεδο του ολοκληρωμένου προϊόντος με ψηφιακά στοιχεία.

Παράδειγμα 61: κατασκευαστής θέτει σε κυκλοφορία στην αγορά ενοποιημένη σουίτα ασφάλειας που συνδυάζει πολλαπλές μονάδες, συμπεριλαμβανομένων συστήματος SIEM, συστήματος ανίχνευσης εισβολών και μονάδας ανάλυσης. Ο κατασκευαστής προσφέρει επίσης τις εν λόγω μονάδες για χωριστές συνδρομές. Στο σενάριο αυτό, κάθε μονάδα αποτελεί διακριτό προϊόν με ψηφιακά στοιχεία και ταξινομείται με βάση τη δική της βασική λειτουργικότητα. Η μονάδα SIEM υπόκειται στο καθεστώς αξιολόγησης της συμμόρφωσης για σημαντικά προϊόντα με ψηφιακά στοιχεία κλάσης I, καθώς η βασική λειτουργικότητά της είναι «Συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM)». Το σύστημα ανίχνευσης εισβολών υπόκειται στο καθεστώς αξιολόγησης της συμμόρφωσης για σημαντικά προϊόντα με ψηφιακά στοιχεία κλάσης II, καθώς η βασική λειτουργικότητά του είναι «Τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών». Η μονάδα ανάλυσης υπόκειται στο καθεστώς αξιολόγησης της συμμόρφωσης για «κανονικά» προϊόντα με ψηφιακά στοιχεία, δεδομένου ότι η βασική της λειτουργικότητα δεν ανήκει στην κατηγορία σημαντικών ή κρίσιμων προϊόντων.

146. Η μη συμμόρφωση με τις υποχρεώσεις που ορίζονται στο άρθρο 32 του κανονισμού για την κυβερνοανθεκτικότητα μπορεί να επισύρει διοικητικά πρόστιμα σύμφωνα με το άρθρο 64 παράγραφος 3.

6.2. Αξιολόγηση της συμμόρφωσης για σημαντικά και κρίσιμα προϊόντα με ψηφιακά στοιχεία

147. Μόλις ο κατασκευαστής καθορίσει τη βασική λειτουργικότητα του προϊόντος του με ψηφιακά στοιχεία, πρέπει να εφαρμόσει μία από τις εφαρμοστέες διαδικασίες αξιολόγησης της συμμόρφωσης. Ο κατασκευαστής πρέπει να διασφαλίζει ότι το προϊόν με ψηφιακά στοιχεία στο σύνολό του πληροί τις ουσιώδεις απαιτήσεις, λαμβάνοντας υπόψη, κατά περίπτωση, την ασφάλεια των δομοστοιχείων ή των λειτουργιών που ενσωματώνονται σε αυτό.

148. Η εφαρμογή αυστηρότερης διαδικασίας αξιολόγησης της συμμόρφωσης, με τη συμμετοχή τρίτου (με βάση την ενότητα Β +Γ, την ενότητα Η ή τα καθεστώτα πιστοποίησης της κυβερνοασφάλειας) είναι υποχρεωτική για σημαντικά προϊόντα με ψηφιακά στοιχεία κλάσης ΙΙ (με εξαίρεση εκείνα που χαρακτηρίζονται ως ελεύθερο λογισμικό ανοικτού κώδικα, σύμφωνα με το άρθρο 32 παράγραφος 5) και για κρίσιμα προϊόντα με ψηφιακά στοιχεία ([24]). Αντιθέτως, τα σημαντικά προϊόντα με ψηφιακά στοιχεία κλάσης Ι (με εξαίρεση εκείνα που χαρακτηρίζονται ως ελεύθερο λογισμικό ανοικτού κώδικα, σύμφωνα με το άρθρο 32 παράγραφος 5) απαιτείται να υποβάλλονται σε διαδικασία αξιολόγησης της συμμόρφωσης από τρίτους μόνο εάν ο κατασκευαστής δεν έχει εφαρμόσει ή έχει εφαρμόσει μόνο εν μέρει σχετικά εναρμονισμένα πρότυπα των οποίων τα στοιχεία αναφοράς έχουν δημοσιευθεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* (στο εξής: εναρμονισμένα πρότυπα), κοινές προδιαγραφές ή ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας σε επίπεδο διασφάλισης τουλάχιστον «σημαντικό» ([25]).

149. Ως εκ τούτου, προκειμένου ένα σημαντικό προϊόν με ψηφιακά στοιχεία κλάσης Ι να είναι επιλέξιμο για τη διαδικασία εσωτερικού ελέγχου, i) πρέπει να εφαρμόζονται όλες οι εφαρμοστέες απαιτήσεις σχετικού εναρμονισμένου προτύπου· και ii) το πεδίο εφαρμογής του προτύπου πρέπει να καλύπτει τουλάχιστον όλους τους κινδύνους κυβερνοασφάλειας που συνδέονται με τη βασική λειτουργικότητα του εν λόγω προϊόντος.

150. Το πεδίο εφαρμογής του προϊόντος με ψηφιακά στοιχεία μπορεί να είναι ευρύτερο από το πεδίο εφαρμογής που προβλέπεται από το σχετικό εναρμονισμένο πρότυπο και οι εν λόγω πρόσθετες λειτουργίες ενδέχεται να παρουσιάζουν διαφορετικούς ή πρόσθετους κινδύνους για την κυβερνοασφάλεια. Ο κατασκευαστής υποχρεούται πάντα να διενεργεί εκτίμηση κινδύνων σύμφωνα με το άρθρο 13 παράγραφος 2 και, κατά συνέπεια, θα πρέπει να ελέγχει αν η εφαρμογή εναρμονισμένου προτύπου καλύπτει όλους τους κινδύνους που συνδέονται με το προϊόν με ψηφιακά στοιχεία. Όταν η εφαρμογή του προτύπου δεν καλύπτει όλους τους κινδύνους, ο κατασκευαστής θα πρέπει να διασφαλίζει με άλλα μέσα ότι το προϊόν του με ψηφιακά στοιχεία συμμορφώνεται με τις ουσιώδεις απαιτήσεις.

151. Ως εκ τούτου, εάν ο κατασκευαστής σημαντικού προϊόντος με ψηφιακά στοιχεία κλάσης Ι εφαρμόζει σχετικό εναρμονισμένο πρότυπο που καλύπτει τους κινδύνους που συνδέονται με τη βασική λειτουργικότητα του εν λόγω προϊόντος, μπορεί να αποφασίσει να χρησιμοποιήσει τη διαδικασία εσωτερικού ελέγχου για να αποδείξει τη συμμόρφωση του προϊόντος του. Στο πλαίσιο των δραστηριοτήτων αξιολόγησης της συμμόρφωσης, ο κατασκευαστής θα εξακολουθεί να υποχρεούται να αποδεικνύει ότι αντιμετωπίζονται όλοι οι κίνδυνοι που ισχύουν για το προϊόν του με ψηφιακά στοιχεία. Ως εκ τούτου, όταν υπάρχει χάσμα μεταξύ της κάλυψης του εναρμονισμένου προτύπου και του πεδίου εφαρμογής του προϊόντος με ψηφιακά στοιχεία στο σύνολό του, ο κατασκευαστής εξακολουθεί να πρέπει να τεκμηριώσει ποια πρόσθετα μέτρα έχει θέσει σε εφαρμογή για την αντιμετώπιση των εν λόγω κινδύνων.

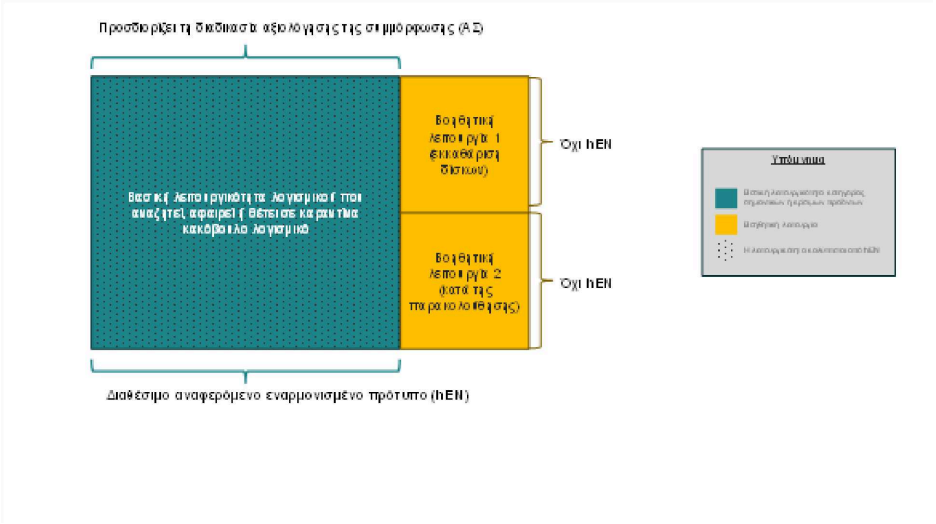
Παράδειγμα 62: Αντικό λογισμικό διαθέτει τη βασική λειτουργικότητα λογισμικού που αναζητεί, αφαιρεί ή θέτει σε καραντίνα κακόβουλο λογισμικό, όπως περιγράφεται στο παράρτημα Ι σημείο 4 του εκτελεστικού κανονισμού (ΕΕ) 2025/2392. Το εν λόγω προϊόν με ψηφιακά στοιχεία περιλαμβάνει επίσης πρόσθετα χαρακτηριστικά, δηλαδή λειτουργία εκκαθάρισης δίσκων και λειτουργία κατά της παρακολούθησης που προστατεύει τον χρήστη κατά την πλοήγηση στο διαδίκτυο. Ο κατασκευαστής διενεργεί εκτίμηση κινδύνων που καλύπτει το προϊόν με ψηφιακά στοιχεία στο σύνολό του, συμπεριλαμβανομένων της βασικής λειτουργικότητας του αντικού λογισμικού, της λειτουργίας εκκαθάρισης δίσκων και της λειτουργίας κατά της παρακολούθησης. Εφαρμόζει εναρμονισμένο πρότυπο που καλύπτει τους κινδύνους που συνδέονται με τη βασική λειτουργικότητα του αντικού λογισμικού, καθώς και πρόσθετα μέτρα για την αντιμετώπιση των κινδύνων που απορρέουν από πρόσθετες λειτουργίες. Ο κατασκευαστής επιτρέπεται να χρησιμοποιεί τη διαδικασία εσωτερικού ελέγχου για την αξιολόγηση της συμμόρφωσής του, η οποία καλύπτει το προϊόν με ψηφιακά στοιχεία στο σύνολό του, συμπεριλαμβανομένων της λειτουργίας εκκαθάρισης δίσκων και της λειτουργίας κατά της παρακολούθησης.

([24]) Αυτό ισχύει επίσης κατά τη χρήση ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας με επίπεδο διασφάλισης τουλάχιστον «σημαντικό», καθώς απαιτείται η συμμετοχή τρίτου οργανισμού πιστοποίησης.

([25]) Για λόγους συντομίας, το υπόλοιπο του παρόντος τμήματος αναφέρεται μόνο σε εναρμονισμένα πρότυπα των οποίων τα στοιχεία αναφοράς έχουν δημοσιευθεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*. Ωστόσο, η ίδια καθοδήγηση ισχύει επίσης για τις κοινές προδιαγραφές που θεσπίζονται σύμφωνα με το άρθρο 27 παράγραφος 2 και για τα ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας, όταν αυτό ορίζεται από την Επιτροπή μέσω κατ' εξουσιοδότηση πράξεων σύμφωνα με το άρθρο 27 παράγραφος 9.

Διάγραμμα 6

Απεικόνιση του τρόπου με τον οποίο η χρήση προτύπου στο οποίο γίνεται αναφορά και το οποίο καλύπτει μόνο τη βασική λειτουργικότητα καθορίζει την εφαρμοστέα διαδικασία αξιολόγησης της συμμόρφωσης



152. Αυτό ισχύει επίσης όταν το προϊόν με ψηφιακά στοιχεία ενσωματώνει πρόσθετη λειτουργία η οποία είναι η ίδια λειτουργία άλλου σημαντικού ή κρίσιμου προϊόντος με ψηφιακά στοιχεία. Στην πραγματικότητα, είναι η βασική λειτουργικότητα του προϊόντος με ψηφιακά στοιχεία στο σύνολό του και όχι η λειτουργικότητα των ενσωματωμένων δομοστοιχείων μεμονωμένα εκείνη που καθορίζει αν το προϊόν με ψηφιακά στοιχεία ανήκει στην κατηγορία σημαντικών ή κρίσιμων προϊόντων (και, ως εκ τούτου, στο εφαρμοστέο καθεστώς αξιολόγησης της συμμόρφωσης). Για παράδειγμα, εάν ένα προϊόν με ψηφιακά στοιχεία έχει τη βασική λειτουργικότητα σημαντικού προϊόντος με ψηφιακά στοιχεία κλάσης Ι, το εν λόγω προϊόν στο σύνολό του υπόκειται στο καθεστώς αξιολόγησης της συμμόρφωσης που ισχύει για σημαντικά προϊόντα με ψηφιακά στοιχεία κλάσης Ι, παρόλο που ενσωματώνει ένα δομοστοιχείο το οποίο αποτελεί το ίδιο κρίσιμο προϊόν με ψηφιακά στοιχεία. Στις περιπτώσεις αυτές, όταν ο κατασκευαστής εφαρμόζει εναρμονισμένο πρότυπο που καλύπτει τους κινδύνους που συνδέονται με τη βασική λειτουργικότητα του εν λόγω προϊόντος, επιτρέπεται να κάνει χρήση της διαδικασίας εσωτερικού ελέγχου.

Παράδειγμα 63: Προϊόν υλισμικού με ψηφιακά στοιχεία έχει τη βασική λειτουργικότητα δρομολογητή, όπως περιγράφεται στο παράρτημα Ι σημείο 12 του εκτελεστικού κανονισμού (ΕΕ) 2025/2392. Το εν λόγω προϊόν με ψηφιακά στοιχεία περιλαμβάνει επίσης πρόσθετες λειτουργίες, συμπεριλαμβανομένων των δυνατοτήτων τείχους προστασίας, καθώς ενσωματώνει δομοστοιχείο τείχους προστασίας. Ο κατασκευαστής διενεργεί εκτίμηση κινδύνων που καλύπτει το προϊόν με ψηφιακά στοιχεία στο σύνολό του, συμπεριλαμβανομένης της βασικής λειτουργικότητας δρομολογητή και της λειτουργικότητας τείχους προστασίας. Εφαρμόζει εναρμονισμένο πρότυπο που καλύπτει τους κινδύνους οι οποίοι συνδέονται με τη βασική λειτουργικότητα του δρομολογητή, καθώς και πρόσθετα μέτρα για την αντιμετώπιση των κινδύνων που απορρέουν από πρόσθετες λειτουργίες. Για παράδειγμα, ο κατασκευαστής μπορεί να εφαρμόζει το εναρμονισμένο πρότυπο για τα τείχη προστασίας για να καλύπτει τους κινδύνους που συνδέονται με τη λειτουργικότητα του τείχους προστασίας. Ο κατασκευαστής επιτρέπεται να χρησιμοποιεί τη διαδικασία εσωτερικού ελέγχου για την αξιολόγηση της συμμόρφωσής του, η οποία καλύπτει το προϊόν με ψηφιακά στοιχεία στο σύνολό του, συμπεριλαμβανομένης της λειτουργικότητας του τείχους προστασίας.

6.3. Συνέπειες για το τεκμήριο συμμόρφωσης

153. Το άρθρο 27 παράγραφος 1 του κανονισμού για την κυβερνοανθεκτικότητα ορίζει ότι τα προϊόντα με ψηφιακά στοιχεία και οι διαδικασίες που εφαρμόζει ο κατασκευαστής που συμμορφώνονται με εναρμονισμένα πρότυπα ή μέρη τους, τα στοιχεία αναφοράς των οποίων έχουν δημοσιευθεί στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, τεκμαίρεται ότι συμμορφώνονται προς τις ουσιώδεις απαιτήσεις του κανονισμού για την κυβερνοανθεκτικότητα τις οποίες αφορούν τα εν λόγω πρότυπα ή τα μέρη αυτών ([26]). Το άρθρο 27 παράγραφος 5 επεκτείνει το ίδιο τεκμήριο συμμόρφωσης σε προϊόντα

([26]) Όπως αναφέρεται σαφώς στο σημείο 4.1.2.2 του Γαλάζιου Οδηγού, «[σ]τη νομοθεσία εναρμόνισης για τους κινδύνους [...] ο κατασκευαστής διατηρεί πάντα, ακόμα και όταν εφαρμόζει εναρμονισμένα πρότυπα τα στοιχεία αναφοράς των οποίων δημοσιεύονται στην Επίσημη Εφημερίδα της *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, την πλήρη ευθύνη για την αξιολόγηση του συνόλου των κινδύνων που παρουσιάζει το εν λόγω προϊόν, ώστε να καθορίζεται ποιες είναι οι σχετικές βασικές (ή άλλες) απαιτήσεις. Έπειτα από αυτή την αξιολόγηση, ο κατασκευαστής μπορεί να επιλέξει να εφαρμόσει τεχνικές προδιαγραφές που περιλαμβάνονται σε εναρμονισμένα πρότυπα τα στοιχεία αναφοράς των οποίων δημοσιεύονται στην Επίσημη Εφημερίδα της *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* για την υλοποίηση "μέτρων μείωσης του κινδύνου", τα οποία καθορίζονται μέσω των εναρμονισμένων προτύπων».

με ψηφιακά στοιχεία και διαδικασίες που εφαρμόζει ο κατασκευαστής τα οποία συμμορφώνονται με τις κοινές προδιαγραφές που θεσπίζονται από την Επιτροπή μέσω εκτελεστικών πράξεων· το δε άρθρο 27 παράγραφος 8 θεσπίζει το τεκμήριο συμμόρφωσης για προϊόντα με ψηφιακά στοιχεία και διαδικασίες που εφαρμόζει ο κατασκευαστής για τα οποία έχει εκδοθεί δήλωση συμμόρφωσης ΕΕ ή πιστοποιητικό στο πλαίσιο ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας που έχει εγκριθεί σύμφωνα με τον κανονισμό (ΕΕ) 2019/881, εάν αυτό έχει προσδιοριστεί μέσω κατ' εξουσιοδότηση πράξεων σύμφωνα με το άρθρο 27 παράγραφος 9 ([27]).

154. Ως εκ τούτου, όταν ο κατασκευαστής εφαρμόζει εναρμονισμένο πρότυπο του οποίου τα στοιχεία αναφοράς έχουν δημοσιευθεί στην Επίσημη Εφημερίδα της ΕΕ, επωφελείται από τεκμήριο συμμόρφωσης για τους κινδύνους που καλύπτονται από το εν λόγω πρότυπο. Αυτό μπορεί να συμβεί, για παράδειγμα, όταν το εναρμονισμένο πρότυπο στο οποίο γίνεται αναφορά αντιμετωπίζει όλους τους κινδύνους που συνδέονται με τη βασική λειτουργικότητα προϊόντος με ψηφιακά στοιχεία και δεν υπάρχουν πρόσθετες λειτουργίες που παρουσιάζουν κινδύνους κυβερνοασφάλειας. Για παράδειγμα, αναμένεται ότι το εναρμονισμένο πρότυπο για τους δρομολογητές θα αντιμετωπίζει τουλάχιστον τους κινδύνους που συνδέονται με τη βασική λειτουργικότητα των εν λόγω προϊόντων με ψηφιακά στοιχεία. Εάν ένα τέτοιο προϊόν δεν περιέχει πρόσθετες λειτουργίες ή εάν αυτές οι πρόσθετες λειτουργίες δεν παρουσιάζουν κινδύνους που δεν καλύπτονται από το πρότυπο, το προϊόν με ψηφιακά στοιχεία μπορεί να επωφεληθεί από το τεκμήριο συμμόρφωσης.

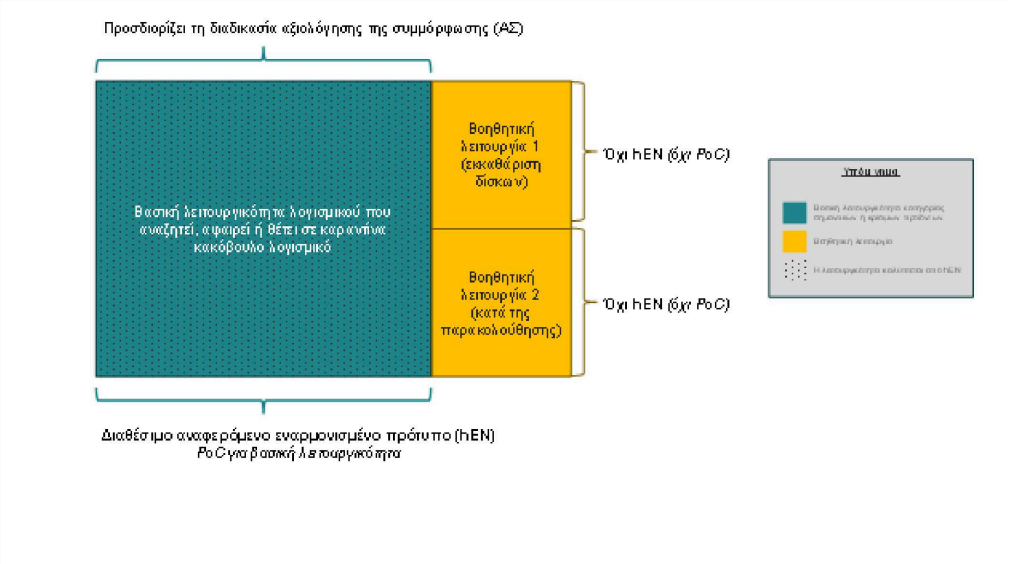
155. Στις περιπτώσεις που εξετάζονται στα σημεία 151 και 152, ο κατασκευαστής επιτρέπεται να χρησιμοποιεί τη διαδικασία εσωτερικού ελέγχου, διότι το εναρμονισμένο πρότυπο καλύπτει τους κινδύνους που συνδέονται με τη βασική λειτουργικότητα του προϊόντος με ψηφιακά στοιχεία. Ωστόσο, τα προϊόντα με ψηφιακά στοιχεία που περιγράφονται στα εν λόγω παραδείγματα μπορεί να είναι ευρύτερα από το πεδίο εφαρμογής των εναρμονισμένων προτύπων και οι πρόσθετες λειτουργίες ενδέχεται να παρουσιάζουν κινδύνους κυβερνοασφάλειας που δεν αντιμετωπίζονται από το εν λόγω εναρμονισμένο πρότυπο. Ως εκ τούτου, τα εν λόγω προϊόντα με ψηφιακά στοιχεία ενδέχεται να μην επωφελούνται από τεκμήριο συμμόρφωσης για τις εν λόγω πρόσθετες λειτουργίες.

Παράδειγμα 64: Αντικό λογισμικό διαθέτει τη βασική λειτουργικότητα λογισμικού που αναζητεί, αφαιρεί ή θέτει σε καραντίνα κακόβουλο λογισμικό και οι κίνδυνοι που συνδέονται με την εν λόγω βασική λειτουργικότητα καλύπτονται από το εναρμονισμένο πρότυπο. Το εν λόγω προϊόν με ψηφιακά στοιχεία περιλαμβάνει επίσης πρόσθετες λειτουργίες, δηλαδή λειτουργία εκκαθάρισης δίσκων και λειτουργία κατά της παρακολούθησης που προστατεύει τον χρήστη κατά την πλοήγηση στο διαδίκτυο, των οποίων οι κίνδυνοι δεν καλύπτονται από το εναρμονισμένο πρότυπο. Εάν εφαρμόζεται το εναρμονισμένο πρότυπο, ο κατασκευαστής επιτρέπεται να κάνει χρήση της διαδικασίας εσωτερικού ελέγχου για την αξιολόγηση της συμμόρφωσης. Θα επωφεληθεί από το τεκμήριο συμμόρφωσης για τους κινδύνους που συνδέονται με τη βασική λειτουργικότητα του εν λόγω προϊόντος, αλλά όχι για τους κινδύνους που συνδέονται με πρόσθετες λειτουργίες.

([27]) Όπως ανωτέρω, για λόγους συντομίας, το υπόλοιπο του παρόντος τμήματος αναφέρεται μόνο σε εναρμονισμένα πρότυπα των οποίων τα στοιχεία αναφοράς έχουν δημοσιευθεί στην Επίσημη Εφημερίδα της *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*. Ωστόσο, η ίδια καθοδήγηση ισχύει και για τις κοινές προδιαγραφές και τα ευρωπαϊκά καθεστώτα πιστοποίησης της κυβερνοασφάλειας.

Διάγραμμα 7

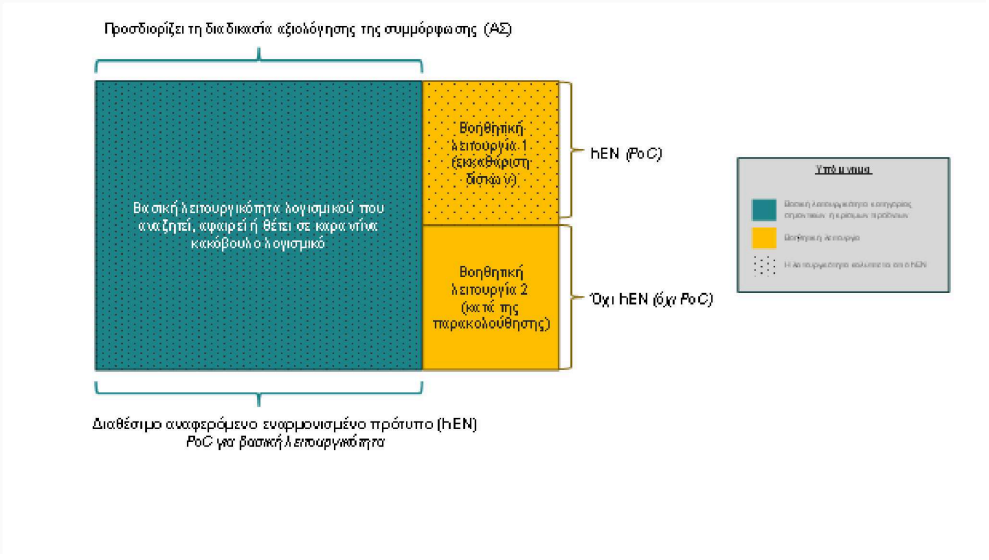
Το εναρμονισμένο πρότυπο εξασφαλίζει τεκμήριο συμμόρφωσης για τη βασική λειτουργικότητα, καθώς αντιμετωπίζει όλους τους κινδύνους που συνδέονται με την εν λόγω βασική λειτουργικότητα, αλλά όχι για τις βοηθητικές λειτουργίες



Παράδειγμα 65: Στο ίδιο σενάριο με το προηγούμενο παράδειγμα, το εναρμονισμένο πρότυπο έχει πλέον επικαιροποιηθεί ώστε να καλύπτει επίσης τους κινδύνους που συνδέονται με μία από τις πρόσθετες λειτουργίες, δηλαδή τη λειτουργία εκκαθάρισης δίσκων, αλλά όχι την άλλη λειτουργία (δηλαδή τη λειτουργία κατά της παρακολούθησης). Εάν εφαρμόζεται το εναρμονισμένο πρότυπο, ο κατασκευαστής επιτρέπεται να κάνει χρήση της διαδικασίας εσωτερικού ελέγχου για την αξιολόγηση της συμμόρφωσης. Θα επωφεληθεί από το τεκμήριο συμμόρφωσης για τους κινδύνους που συνδέονται με τη βασική λειτουργικότητα του εν λόγω προϊόντος και για τη λειτουργία εκκαθάρισης δίσκων, αλλά όχι για τους κινδύνους που σχετίζονται με τη λειτουργία κατά της παρακολούθησης.

Διάγραμμα 8

Το εναρμονισμένο πρότυπο διασφαλίζει το τεκμήριο συμμόρφωσης για τη βασική λειτουργικότητα και τη βοηθητική λειτουργία 1, καθώς αντιμετωπίζει όλους τους κινδύνους που συνδέονται με τις δύο αυτές λειτουργίες, αλλά όχι για τη βοηθητική λειτουργία 2



7. **ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΩΝ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΕΝΣΩΜΑΤΩΣΗ ΠΡΟΪΟΝΤΩΝ ΜΕ ΨΗΦΙΑΚΑ ΣΤΟΙΧΕΙΑ ΚΑΙ ΔΟΜΟΣΤΟΙΧΕΙΩΝ**

7.1. **Σχετικά με την αξιολόγηση και την αντιμετώπιση των κινδύνων κυβερνοασφάλειας**

156. Η εκτίμηση κινδύνων για την κυβερνοασφάλεια που προβλέπεται στο άρθρο 13 παράγραφος 2 του κανονισμού για την κυβερνοανθεκτικότητα απαιτεί από τους κατασκευαστές να εντοπίζουν τους σχετικούς κινδύνους και να αξιολογούν τις δυνητικές επιπτώσεις τους στο προϊόν με ψηφιακά στοιχεία. Οι κατασκευαστές πρέπει επίσης να εφαρμόζουν κατάλληλα μέτρα για την αντιμετώπιση των εν λόγω κινδύνων, σύμφωνα με τις ουσιώδεις απαιτήσεις του παραρτήματος Ι.

157. Στο πλαίσιο της διαχείρισης κινδύνων σε επίπεδο οργανισμού, οι κίνδυνοι αξιολογούνται συνήθως με βάση τα κριτήρια αποδοχής που προκύπτουν από τους εσωτερικούς στόχους ή τη διάθεση ανάληψης κινδύνου του οργανισμού. Αντιθέτως, στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα, ο υπολειπόμενος κίνδυνος κυβερνοασφάλειας θα πρέπει να αξιολογείται υπό το πρίσμα της απαίτησης το προϊόν με ψηφιακά στοιχεία που τίθεται σε κυκλοφορία στην αγορά να διασφαλίζει κατάλληλο επίπεδο κυβερνοασφάλειας με βάση τους κινδύνους, λαμβανομένων υπόψη του επιδιωκόμενου σκοπού του και της ευλόγως προβλέψιμης χρήσης του.

158. Κατά συνέπεια, η εσωτερική ανοχή κινδύνου, η εμπορική στρατηγική ή απλές εκτιμήσεις κόστους του κατασκευαστή δεν έχουν σημασία για τον προσδιορισμό του αν έχουν αντιμετωπιστεί οι κίνδυνοι. Για τους σκοπούς του άρθρου 13 παράγραφοι 2 και 3, οι κατασκευαστές πρέπει να είναι σε θέση να προσδιορίζουν αν οι εντοπισθέντες κίνδυνοι κυβερνοασφάλειας αντιμετωπίζονται επαρκώς μέσω της εφαρμογής των ουσιωδών απαιτήσεων του παραρτήματος Ι μέρος Ι, υπό το πρίσμα του επιδιωκόμενου σκοπού, της ευλόγως προβλέψιμης χρήσης και των όρων χρήσης, συμπεριλαμβανομένων, κατά περίπτωση, του επιχειρησιακού περιβάλλοντος (για παράδειγμα, των προβλεπόμενων χρηστών του προϊόντος με ψηφιακά στοιχεία) και των περιουσιακών στοιχείων που πρέπει να προστατευθούν, λαμβανομένου υπόψη του χρονικού διαστήματος που αναμένεται να χρησιμοποιηθεί το προϊόν με ψηφιακά στοιχεία.

159. Ο υπολειπόμενος κίνδυνος κυβερνοασφάλειας είναι εγγενές αποτέλεσμα της εκτίμησης κινδύνων και της αντιμετώπισης κινδύνων. Αναγνωρίζεται ότι οι κίνδυνοι κυβερνοασφάλειας δεν μπορούν, στην πράξη, να εξαλειφθούν πλήρως. Ωστόσο, η ύπαρξη υπολειπόμενου κινδύνου δεν συνεπάγεται ότι οποιοσδήποτε κίνδυνος μπορεί να γίνει αποδεκτός κατά τη διακριτική ευχέρεια του κατασκευαστή. Ένα προϊόν με ψηφιακά στοιχεία μπορεί να τεθεί σε κυκλοφορία στην αγορά μόνο όταν οι υπολειπόμενοι κίνδυνοι, αφού ληφθούν κατάλληλα μέτρα, αντιμετωπίζονται επαρκώς μέσω της εφαρμογής των ουσιωδών απαιτήσεων, λαμβανομένων υπόψη του επιδιωκόμενου σκοπού και της ευλόγως προβλέψιμης χρήσης του προϊόντος με ψηφιακά στοιχεία.

160. Σύμφωνα με το άρθρο 13 παράγραφος 3, όταν εντοπίζονται κίνδυνοι κυβερνοασφάλειας, οι κατασκευαστές υποχρεούνται να τους αντιμετωπίζουν μέσω κατάλληλων μέτρων, μεταξύ άλλων σε επίπεδο προϊόντος. Ανάλογα με τις περιστάσεις, στα εν λόγω μέτρα μπορούν να περιλαμβάνονται, για παράδειγμα, η μείωση της επιφάνειας επίθεσης, η εφαρμογή τεχνικών διασφαλίσεων, ο περιορισμός ή η προσαρμογή της λειτουργικότητας ή ο ακριβέστερος καθορισμός του επιδιωκόμενου σκοπού του προϊόντος με ψηφιακά στοιχεία. Οι κατασκευαστές μπορούν επίσης να λαμβάνουν μέτρα για τη διαμόρφωση της ευλόγως προβλέψιμης χρήσης του προϊόντος με ψηφιακά στοιχεία, για παράδειγμα μέσω της ενημέρωσης σχετικά με τον κίνδυνο, της καθοδήγησης των χρηστών ή του σχεδιασμού της διεπαφής χρήστη, προκειμένου να κατευθύνουν τη συμπεριφορά των χρηστών προς ασφαλή πρότυπα χρήσης.

161. Στο κανονισμό για την κυβερνοανθεκτικότητα δεν προβλέπεται η μεταβίβαση του κινδύνου ή της ευθύνης για την κυβερνοασφάλεια στους χρήστες ή σε τρίτους με σκοπό να αντισταθμίζονται οι ελλείψεις στον σχεδιασμό των προϊόντων ή να αιτιολογείται η μη αντιμετώπιση των κινδύνων κυβερνοασφάλειας. Η υποχρέωση θέσης ασφαλούς προϊόντος με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά και απόδειξης της συμμόρφωσης με τις ουσιώδεις απαιτήσεις εξακολουθεί να βαρύνει τον κατασκευαστή.

162. Οι πληροφορίες και οι οδηγίες που παρέχονται στους χρήστες μπορούν να χρησιμοποιηθούν για την υποστήριξη της ασφαλούς εγκατάστασης και λειτουργίας του προϊόντος με ψηφιακά στοιχεία, μεταξύ άλλων όταν ο κατασκευαστής έχει επιλέξει να περιορίσει τον προβλεπόμενο σκοπό του εν λόγω προϊόντος σε αξιόπιστα περιβάλλοντα, καθώς και για την ενημέρωση των χρηστών για τους υπολειπόμενους κινδύνους, με τρόπο κατάλληλο για τη φύση του προϊόντος με ψηφιακά στοιχεία και τους προβλεπόμενους χρήστες του.

Παράδειγμα 66: Κατασκευαστής αναπτύσσει βιομηχανικό αισθητήρα για χρήση σε αξιόπιστα περιβάλλοντα. Για την ορθή εκτέλεση της λειτουργικότητας του αισθητήρα, ο κατασκευαστής δεν εφαρμόζει μέτρα προστασίας από φυσικές επιθέσεις στον ίδιο τον αισθητήρα. Για τον μετριασμό των σχετικών κινδύνων που προσδιορίζονται στην εκτίμηση κινδύνων, ο κατασκευαστής περιορίζει τον επιδιωκόμενο σκοπό του αισθητήρα ώστε να χρησιμοποιείται μόνο σε αξιόπιστα περιβάλλοντα όπου αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση στο προϊόν με ψηφιακά στοιχεία. Οι πληροφορίες και οι οδηγίες προς τους χρήστες παρέχουν σαφείς πληροφορίες σχετικά με τους εν λόγω περιορισμούς όσον αφορά χρήση του αισθητήρα, με τρόπο κατάλληλο για τη φύση του προϊόντος με ψηφιακά στοιχεία και τους προβλεπόμενους χρήστες του.

Παράδειγμα 67: Κατασκευαστής αναπτύσσει εφαρμογή λογισμικού για επαγγελματική χρήση σε υπό διαχείριση επιτραπέζιες και κινητές συσκευές. Η εφαρμογή επεξεργάζεται τοπικά αποθηκευμένα ευαίσθητα δεδομένα και περιεχόμενο που παράγεται από τους χρήστες. Κατά τη διάρκεια της εκτίμησης κινδύνων, ο κατασκευαστής εντοπίζει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης στα εν λόγω δεδομένα εάν αποθηκεύονται σε ακρυπτογράφητο κείμενο επί της συσκευής. Αντί να σχεδιάσει και να εφαρμόσει έναν ιδιόκτητο μηχανισμό κρυπτογράφησης εντός της ίδιας της εφαρμογής, ο κατασκευαστής επιλέγει να βασιστεί στις λειτουργίες κρυπτογράφησης και διαχείρισης κλειδιών που παρέχονται εγγενώς από το λειτουργικό σύστημα στο οποίο προορίζεται να λειτουργήσει η εφαρμογή, καθώς οι ενσωματωμένες κρυπτογραφικές υπηρεσίες του λειτουργικού συστήματος είναι ώριμες και συντηρούνται τακτικά.

163. Όταν η εκτίμηση κινδύνων για την κυβερνοασφάλεια εντοπίζει κινδύνους που δεν μπορούν να αντιμετωπιστούν επαρκώς με κατάλληλα μέτρα, η συμμόρφωση με τον κανονισμό για την κυβερνοανθεκτικότητα μπορεί να απαιτεί αλλαγές στον σχεδιασμό, στη λειτουργικότητα ή στον επιδιωκόμενο σκοπό του προϊόντος με ψηφιακά στοιχεία. Εκτιμήσεις που αφορούν αποκλειστικά το κόστος ή την εμπορική σκοπιμότητα δεν συνιστούν επαρκείς λόγους για τη μη αντιμετώπιση των εν λόγω κινδύνων εφόσον αυτό θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκπληρώσει τις ουσιώδεις απαιτήσεις.

7.2. Σχετικά με τον σχεδιασμό, την ανάπτυξη και την παραγωγή προϊόντων με τρόπο ώστε να εγγυώνται κατάλληλο επίπεδο κυβερνοασφάλειας βάσει των κινδύνων.

164. Με βάση την ουσιώδη απαίτηση κυβερνοασφάλειας που αναφέρεται στο παράρτημα Ι μέρος Ι σημείο 1 του κανονισμού για την κυβερνοανθεκτικότητα προβλέπεται ότι τα προϊόντα με ψηφιακά στοιχεία σχεδιάζονται, αναπτύσσονται και παράγονται κατά τρόπο ώστε να διασφαλίζουν κατάλληλο επίπεδο κυβερνοασφάλειας βάσει των κινδύνων.

165. Η εν λόγω ουσιώδης απαίτηση αποσκοπεί στην αντιμετώπιση όλων των κινδύνων κυβερνοασφάλειας που έχουν προσδιοριστεί στο πλαίσιο της εκτίμησης κινδύνων κυβερνοασφάλειας. Ειδικότερα, η απαίτηση αφορά κινδύνους κυβερνοασφάλειας που δεν αντιμετωπίζονται επαρκώς με άλλον τρόπο στο πλαίσιο της εφαρμογής των ουσιωδών απαιτήσεων του παραρτήματος Ι μέρος Ι πλην του σημείου 1. Αυτή η ουσιώδης απαίτηση διαφέρει από τη νομική υποχρέωση διενέργειας εκτίμησης κινδύνων κυβερνοασφάλειας, η οποία πρέπει να διενεργείται σύμφωνα με το άρθρο 13 παράγραφος 2.

166. Όταν όλοι οι σχετικοί κίνδυνοι κυβερνοασφάλειας που σχετίζονται με προϊόν με ψηφιακά στοιχεία αντιμετωπίζονται με την εφαρμογή κατάλληλων μέτρων για την αντιμετώπιση των εφαρμοστέων ουσιωδών απαιτήσεων εκτός του σημείου 1, θεωρείται ότι πληρούται η ουσιώδης απαίτηση που αναφέρεται στο παράρτημα Ι μέρος Ι σημείο 1. Αντιθέτως, όταν η εκτίμηση κινδύνων για την κυβερνοασφάλεια εντοπίζει πρόσθετους κινδύνους που δεν αντιμετωπίζονται πλήρως από τα εν λόγω μέτρα, οι κατασκευαστές υποχρεούνται να εφαρμόζουν κατάλληλα μέτρα στο προϊόν με ψηφιακά στοιχεία για την αντιμετώπιση των εν λόγω κινδύνων, ώστε να συμμορφώνονται με την ουσιώδη απαίτηση που αναφέρεται στο παράρτημα Ι μέρος Ι σημείο 1. Στην πράξη, στις περισσότερες περιπτώσεις, η συμμόρφωση με τις λοιπές ουσιώδεις απαιτήσεις αναμένεται να έχει ως αποτέλεσμα τη συμμόρφωση με την εν λόγω απαίτηση.

7.3. Εκτίμηση κινδύνων και δέουσα επιμέλεια σε σχέση με εξωτερικές εξαρτήσεις και ενσωματωμένα δομοστοιχεία

167. Ο κανονισμός για την κυβερνοανθεκτικότητα θεσπίζει δύο διακριτές αλλά συμπληρωματικές υποχρεώσεις για τους κατασκευαστές σε σχέση με τη διαχείριση κινδύνων κυβερνοασφάλειας. Πρώτον, βάσει του άρθρου 13 παράγραφος 2 απαιτείται από τους κατασκευαστές να διενεργούν εκτίμηση κινδύνων κυβερνοασφάλειας για το ίδιο το προϊόν με ψηφιακά στοιχεία. Δεύτερον, το άρθρο 13 παράγραφος 5 επιβάλλει την υποχρέωση να επιδεικνύεται η δέουσα επιμέλεια όσον αφορά τα ενσωματωμένα δομοστοιχεία. Από κοινού, οι δύο αυτές υποχρεώσεις έχουν σχεδιαστεί για να διασφαλίζουν ότι το προϊόν με ψηφιακά στοιχεία παραμένει ασφαλές, μεταξύ άλλων όταν βασίζεται σε λύσεις εξ αποστάσεως επεξεργασίας δεδομένων, εξ αποστάσεως υπηρεσίες ή δομοστοιχεία λογισμικού ή υλισμικού τρίτων.

168. Η εκτίμηση κινδύνων για την κυβερνοασφάλεια αφορά τον εντοπισμό και τη διαχείριση σχετικών κινδύνων που ενδέχεται να επηρεάσουν το προϊόν με ψηφιακά στοιχεία, συμπεριλαμβανομένων των κινδύνων που προέρχονται εκτός του ίδιου του προϊόντος, όπως εξωτερικά δίκτυα, περιβαλλοντικοί παράγοντες ή άλλες εξωτερικές πτυχές που ενδέχεται να επηρεάσουν το προϊόν με ψηφιακά στοιχεία ή στις οποίες βασίζεται το προϊόν. Για τους εν λόγω εξωτερικούς κινδύνους, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα δεν απαιτείται από τους κατασκευαστές να ελέγχουν ή να ρυθμίζουν το εξωτερικό περιβάλλον. Αντιθέτως, οι κατασκευαστές υποχρεούνται να εντοπίζουν τους εν λόγω κινδύνους και να τους μετριάζουν μέσω του σχεδιασμού και της ανάπτυξης του ίδιου του προϊόντος με ψηφιακά στοιχεία. Αυτό συνεπάγεται την εφαρμογή των κατάλληλων ουσιωδών απαιτήσεων που ορίζονται στο μέρος Ι του παραρτήματος Ι και, όπου απαιτείται, την παροχή πληροφοριών και οδηγιών στους χρήστες σχετικά με τους κινδύνους ενσωμάτωσης ή εγκατάστασης.

169. Για παράδειγμα, ένας κατασκευαστής μπορεί να εντοπίσει τον κίνδυνο μη εξουσιοδοτημένα πρόσωπα να αποκτήσουν πρόσβαση σε συστήματα υποστηρικτικών λειτουργιών που δεν αποτελούν μέρος του ίδιου του προϊόντος με ψηφιακά στοιχεία κατά τη διάρκεια της λειτουργίας του προϊόντος και να επιχειρήσουν να αποστείλουν κακόβουλες εντολές στο προϊόν με ψηφιακά στοιχεία. Τα εν λόγω συστήματα υποστηρικτικών λειτουργιών, όταν δεν σχεδιάζονται και δεν αναπτύσσονται από τον κατασκευαστή ή υπό την ευθύνη του ή όταν δεν υποστηρίζουν μία από τις λειτουργίες του προϊόντος με ψηφιακά στοιχεία, δεν αποτελούν λύσεις εξ αποστάσεως επεξεργασίας δεδομένων και, ως εκ τούτου, δεν εμπίπτουν στο πεδίο εφαρμογής του προϊόντος με ψηφιακά στοιχεία για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα. Ωστόσο, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα απαιτείται από τον κατασκευαστή να αντιμετωπίζει τον κίνδυνο που ενδέχεται να ενέχουν μέσω μέτρων σε επίπεδο προϊόντος, όπως η απαίτηση κρυπτογραφικής επαλήθευσης ταυτότητας των εξ αποστάσεως εντολών, η επαλήθευση της ακεραιότητας των αλλαγών διαμόρφωσης ή η δημιουργία αρχείων καταγραφής ή ειδοποιήσεων σχετικών με την ασφάλεια όταν εντοπίζεται μη φυσιολογική συμπεριφορά. Ομοίως, σε περίπτωση που ένας κατασκευαστής εντοπίζει κίνδυνο που προκύπτει από τη μη διαθεσιμότητα μιας τέτοιας εξωτερικής υπηρεσίας, για παράδειγμα λόγω διακοπών ρεύματος ή αστοχιών της υποδομής, μπορεί, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα, να απαιτούνται μέτρα μετριασμού σε επίπεδο προϊόντος έναντι των εν λόγω κινδύνων κυβερνοασφάλειας, π.χ. για να διασφαλιστεί ότι η διακοπή ρεύματος δεν έχει ως συνέπεια το προϊόν με ψηφιακά στοιχεία να περιέλθει σε μη ασφαλείς καταστάσεις. Στις περιπτώσεις αυτές, ο κανονισμός για την κυβερνοανθεκτικότητα ρυθμίζει τον τρόπο με τον οποίο το προϊόν με ψηφιακά στοιχεία αντιμετωπίζει τους εν λόγω εξωτερικούς κινδύνους· δεν επιβάλλει υποχρεώσεις σχετικά με τον τρόπο οργάνωσης, στελέχωσης ή λειτουργίας της υποδομής υποστηρικτικών λειτουργιών ούτε αντιμετωπίζει την εν λόγω υποδομή ως μέρος του προϊόντος με ψηφιακά στοιχεία.

170. Η δέουσα επιμέλεια αφορά στοιχεία που αποτελούν μέρος του ίδιου του προϊόντος με ψηφιακά στοιχεία, ιδίως ενσωματωμένα δομοστοιχεία λογισμικού ή υλισμικού που παρέχονται από τρίτους. Οι κατασκευαστές υποχρεούνται να λαμβάνουν κατάλληλα μέτρα για να διασφαλίζουν ότι τα εν λόγω δομοστοιχεία δεν υπονομεύουν τη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία με τις ουσιώδεις απαιτήσεις. Αυτό μπορεί να επιτευχθεί μόνο με τον προσδιορισμό του τι απαιτεί το προϊόν με ψηφιακά στοιχεία από τα δομοστοιχεία του προκειμένου να επιτύχει τους στόχους του για την κυβερνοασφάλεια και μέσω της επαλήθευσης, με βάση τον κίνδυνο, του ότι τα εν λόγω δομοστοιχεία συνάδουν με τις ανάγκες του προϊόντος, όπως αναφέρεται επίσης στην αιτιολογική σκέψη 34.

171. Σύμφωνα με την εκτίμηση κινδύνων για την κυβερνοασφάλεια, ο κατασκευαστής πρέπει να προσδιορίζει τις απαιτήσεις που θα πρέπει να πληροί το ενσωματωμένο δομοστοιχείο. Για παράδειγμα, εάν το προϊόν με ψηφιακά στοιχεία βασίζεται σε κρυπτογραφικές λειτουργίες, μηχανισμούς ενημέρωσης ή ασφαλείς επικοινωνίες που παρέχονται από δομοστοιχείο, ο κατασκευαστής πρέπει, στο πλαίσιο της δέουσας επιμέλειας, να προσδιορίζει τις εν λόγω ανάγκες και να επαληθεύει ότι το δομοστοιχείο τις ικανοποιεί. Τα αποδεικτικά στοιχεία για τον σκοπό αυτόν μπορούν να συνίστανται σε τεκμηρίωση που λαμβάνεται από τον κατασκευαστή του δομοστοιχείου, όπως τεχνικές προδιαγραφές, τεκμηρίωση ασφάλειας ή σχετική τεκμηρίωση συμμόρφωσης ή διασφάλισης. Κατά περίπτωση, ο κατασκευαστής μπορεί επίσης να διενεργεί δοκιμές για να επαληθεύει ότι τα εν λόγω δομοστοιχεία εκτελούν επαρκώς τις σχετικές λειτουργίες. Μολονότι η δέουσα επιμέλεια αποτελεί χωριστή νομική υποχρέωση, υποστηρίζει και ενισχύει την ικανότητα του κατασκευαστή να αποδεικνύει τη συμμόρφωση με τις ουσιώδεις απαιτήσεις για το προϊόν με ψηφιακά στοιχεία στο σύνολό του.

172. Κατά την αξιολόγηση των κινδύνων για το προϊόν με ψηφιακά στοιχεία στο σύνολό του, στοιχεία εκτός του προϊόντος, όπως περιβαλλοντικά στοιχεία, εξωτερικές υποδομές, άλλα συστήματα ή δίκτυα, πρέπει να λαμβάνονται υπόψη στην εκτίμηση κινδύνων κυβερνοασφάλειας και, κατά περίπτωση, να αντιμετωπίζονται μέσω μέτρων σε επίπεδο προϊόντος ώστε να διασφαλίζεται η συμμόρφωση του προϊόντος με ψηφιακά στοιχεία με τις ουσιώδεις απαιτήσεις. Τα δομοστοιχεία που είναι φυσικά ή λογικά ενσωματωμένα στο προϊόν με ψηφιακά στοιχεία, αλλά προέρχονται από τρίτους, πρέπει επίσης να εξετάζονται στο πλαίσιο της εκτίμησης κινδύνων. Ωστόσο, για λόγους συμμόρφωσης, ο κατασκευαστής θα πρέπει να αντιμετωπίζει τα εν λόγω δομοστοιχεία ως εξωτερικά παρεχόμενα δομοστοιχεία των οποίων οι ιδιότητες επαληθεύονται μέσω δέουσας επιμέλειας κατά την ενσωμάτωσή τους, καθώς ο κατασκευαστής ενδέχεται να μην τα έχει επανασχεδιάσει ή αναπτύξει εκ νέου.

173. Η ίδια λογική ισχύει κατά την ανάπτυξη και την ενσωμάτωση των δομοστοιχείων. Όταν ο κατασκευαστής αναπτύσσει ο ίδιος λειτουργίες, πρέπει να εφαρμόζει άμεσα τις ουσιώδεις απαιτήσεις. Όταν ο κατασκευαστής ενσωματώνει δομοστοιχεία που έχουν αναπτυχθεί από άλλους, πρέπει να διασφαλίζει μέσω της δέουσας επιμέλειας ότι τα εν λόγω δομοστοιχεία μπορούν να χρησιμοποιηθούν με τρόπο που να επιτρέπει τη συμμόρφωση του προϊόντος με ψηφιακά στοιχεία στο σύνολό του. Και στις δύο περιπτώσεις, ο στόχος παραμένει ο ίδιος: ότι το προϊόν με ψηφιακά στοιχεία, όπως τίθεται σε κυκλοφορία στην αγορά, επιτυγχάνει κατάλληλο επίπεδο κυβερνοασφάλειας, όπως απαιτείται σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα, λαμβανομένων υπόψη των κινδύνων που προσδιορίζονται στην εκτίμηση κινδύνων για την κυβερνοασφάλεια.

7.4. **Εκ νέου χρήση εκτιμήσεων κινδύνων και εγγράφων τεκμηρίωσης της συμμόρφωσης για οικογένειες προϊόντων με ψηφιακά στοιχεία**

174. Οι κατασκευαστές μπορούν να θέτουν σε κυκλοφορία στην αγορά προϊόντα με ψηφιακά στοιχεία που είναι παρόμοια, για παράδειγμα διαφορετικές παραλλαγές, μοντέλα ή διαμορφώσεις της ίδιας οικογένειας προϊόντων. Όταν τα εν λόγω προϊόντα με ψηφιακά στοιχεία έχουν την ίδια αρχιτεκτονική, τον ίδιο σχεδιασμό που σχετίζεται με την ασφάλεια και τον ίδιο επιδιωκόμενο σκοπό και εκτίθενται στους ίδιους κινδύνους κυβερνοασφάλειας, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα δεν απαιτείται από τους κατασκευαστές να αντιμετωπίζουν κάθε παραλλαγή ως εντελώς χωριστό προϊόν με ψηφιακά στοιχεία για τους σκοπούς της εκτίμησης κινδύνων και της αξιολόγησης της συμμόρφωσης.

175. Στις περιπτώσεις αυτές, υπό την προϋπόθεση ότι όλες οι σχετικές παραλλαγές καλύπτονται επαρκώς όσον αφορά τους σχετικούς κινδύνους και τις ουσιώδεις απαιτήσεις, οι κατασκευαστές μπορούν να βασίζονται: i) σε μία ενιαία εκτίμηση κινδύνων για την κυβερνοασφάλεια που διενεργείται σύμφωνα με το άρθρο 13 παράγραφος 2 του κανονισμού για την κυβερνοανθεκτικότητα· ii) σε ένα ενιαίο σύνολο εγγράφων τεχνικής τεκμηρίωσης (τεχνικό φάκελο)· και iii) σε μία ενιαία διαδικασία αξιολόγησης της συμμόρφωσης. Με αυτόν τον τρόπο καθίσταται επίσης δυνατή η έκδοση μίας ενιαίας δήλωσης συμμόρφωσης ΕΕ για την ομάδα προϊόντων με ψηφιακά στοιχεία, εφόσον προσδιορίζονται σε αυτή με σαφήνεια οι παραλλαγές του προϊόντος στις οποίες εφαρμόζεται.

176. Ο καθοριστικός παράγοντας είναι αν οι διαφορές μεταξύ των παραλλαγών είναι σημαντικές για την κυβερνοασφάλεια. Για τροποποιήσεις που δεν επηρεάζουν τις ιδιότητες κυβερνοασφάλειας του προϊόντος με ψηφιακά στοιχεία, όπως διαφορές στο χρώμα, στον παράγοντα μορφής, στο μέγεθος της μνήμης ή άλλα χαρακτηριστικά που δεν σχετίζονται με την ασφάλεια, δεν απαιτούνται χωριστές εκτιμήσεις κινδύνων ή αξιολογήσεις της συμμόρφωσης. Αντιθέτως, σε ορισμένες περιπτώσεις οι παραλλαγές μπορεί να διαφέρουν με τρόπους που επηρεάζουν την εφαρμογή των ουσιωδών απαιτήσεων, για παράδειγμα μέσω διαφορετικών διεπαφών επικοινωνίας, στοιβών λογισμικού, μηχανισμών ενημέρωσης ή εξ αποστάσεως συνδεσιμότητας. Στις περιπτώσεις αυτές, οι εν λόγω διαφορές πρέπει να αντικατοπτρίζονται στην εκτίμηση κινδύνων και, εφόσον απαιτείται, στην αξιολόγηση της συμμόρφωσης και στον τεχνικό φάκελο.

177. Οι κατασκευαστές παραμένουν υπεύθυνοι να διασφαλίζουν ότι η εκτίμηση κινδύνων και η σχετική τεκμηρίωση αντικατοπτρίζουν με ακρίβεια τα προϊόντα με ψηφιακά στοιχεία που τίθενται σε κυκλοφορία στην αγορά. Όταν μια νέα παραλλαγή δημιουργεί νέους κινδύνους κυβερνοασφάλειας ή μεταβάλλει τον τρόπο εφαρμογής των ουσιωδών απαιτήσεων, η υφιστάμενη εκτίμηση κινδύνων και η τεκμηρίωση της συμμόρφωσης πρέπει να επικαιροποιούνται αναλόγως. Η εξάρτηση από μία ενιαία αξιολόγηση της συμμόρφωσης είναι δυνατή μόνο στον βαθμό που τα προϊόντα με ψηφιακά στοιχεία δεν παρουσιάζουν διαφορές όσον αφορά τις ιδιότητές τους στον τομέα της κυβερνοασφάλειας.

8. **ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ**

178. Στο άρθρο 3 σημείο 1) του κανονισμού για την κυβερνοανθεκτικότητα ως προϊόν με ψηφιακά στοιχεία ορίζεται «κάθε προϊόν λογισμικού ή υλισμικού και οι οικείες λύσεις εξ αποστάσεως επεξεργασίας δεδομένων, συμπεριλαμβανομένων των δομοστοιχείων λογισμικού ή υλισμικού που τίθενται σε κυκλοφορία στην αγορά χωριστά». Υπό το πρίσμα αυτό, ο κατασκευαστής πρέπει να εξετάζει το προϊόν με ψηφιακά στοιχεία στο σύνολό του, συμπεριλαμβανομένων των λύσεων εξ αποστάσεως επεξεργασίας δεδομένων (RDPS). Για παράδειγμα, στο πλαίσιο της απόδειξης ότι το προϊόν με ψηφιακά στοιχεία συμμορφώνεται με τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα I, πρέπει να λαμβάνονται υπόψη οι λύσεις εξ αποστάσεως επεξεργασίας δεδομένων, αρχής γενομένης από την εκτίμηση κινδύνων (άρθρο 13 παράγραφος 2). Το ίδιο ισχύει και κατά την εξέταση των υποχρεώσεων που αφορούν τον κύκλο ζωής, όπως η αναφορά ευπαθειών που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και σοβαρών περιστατικών (άρθρο 14).

179. Σκοπός του παρόντος εγγράφου καθοδήγησης είναι να παράσχει περαιτέρω υποστήριξη στους κατασκευαστές προκειμένου να προσδιορίζουν το αν το προϊόν τους με ψηφιακά στοιχεία διαθέτει λύσεις εξ αποστάσεως επεξεργασίας δεδομένων, όπως ορίζεται στον κανονισμό για την κυβερνοανθεκτικότητα, καθώς και τον τρόπο εκπλήρωσης των σχετικών υποχρεώσεών συμμόρφωσής τους. Μετά από μια αρχική ανάλυση των ορισμών και των αιτιολογικών σκέψεων που παρατίθενται στον κανονισμό για την κυβερνοανθεκτικότητα, το παρόν έγγραφο καθοδήγησης θα περιλαμβάνει ερωτήσεις που θα καθοδηγούν τους κατασκευαστές να διευκρινίζουν αν το προϊόν τους με ψηφιακά στοιχεία περιλαμβάνει λύσεις εξ αποστάσεως επεξεργασίας δεδομένων (βλ. τμήμα *8.1 What is considered a remote data processing solution for a product with digital elements?*). Στη συνέχεια, θα αναλυθούν οι τεχνικές επιπτώσεις των λύσεων εξ αποστάσεως επεξεργασίας δεδομένων και ο τρόπος αξιολόγησης της συμμόρφωσης με τον κανονισμό για την κυβερνοανθεκτικότητα (βλ. τμήμα *8.2 Practical and technical implications of remote data processing solutions and reliance on third-party solutions*).

180. Στην πραγματικότητα, στο άρθρο 3 σημείο 2) η έννοια της «εξ αποστάσεως επεξεργασίας δεδομένων» ορίζεται ως «εξ αποστάσεως επεξεργασία δεδομένων για την οποία το λογισμικό έχει σχεδιαστεί και αναπτυχθεί από τον κατασκευαστή ή υπό την ευθύνη του κατασκευαστή και η απουσία της οποίας θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του». Ως εκ τούτου, οι λύσεις εξ αποστάσεως επεξεργασίας δεδομένων ορίζονται ως τα στοιχεία λογισμικού [«το μέρος ηλεκτρονικού συστήματος πληροφοριών που αποτελείται από κώδικα υπολογιστή», όπως ορίζεται στο άρθρο 3 σημείο 4)] της εξ αποστάσεως επεξεργασίας δεδομένων. Η συγκεκριμένη έννοια δεν αποσκοπεί να συμπεριλαμβάνει, στο πλαίσιο του πεδίου εφαρμογής του προϊόντος με ψηφιακά στοιχεία, το υλισμικό στο οποίο μπορεί να βασίζεται η εξ αποστάσεως επεξεργασία δεδομένων.

181. Στις αιτιολογικές σκέψεις 11 και 12 παρέχονται περαιτέρω εξηγήσεις σχετικά με τον τρόπο με τον οποίο θα πρέπει να ερμηνεύεται η έννοια αυτή. Στην αιτιολογική σκέψη 11 διευκρινίζεται ότι ο στόχος της κάλυψης της λύσης εξ αποστάσεως επεξεργασίας δεδομένων είναι «τα εν λόγω προϊόντα να προστατεύονται επαρκώς στο σύνολό τους από τους κατασκευαστές τους, ανεξάρτητα από το αν τα δεδομένα υποβάλλονται σε επεξεργασία ή αποθηκεύονται τοπικά στη συσκευή του χρήστη ή εξ αποστάσεως από τον κατασκευαστή». Αναφέρεται, επίσης, ότι «οι απαιτήσεις σχετικά με τις λύσεις εξ αποστάσεως επεξεργασίας δεδομένων που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού δεν συνεπάγονται τεχνικά, επιχειρησιακά ή οργανωτικά μέτρα που αποσκοπούν στη διαχείριση των κινδύνων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών του κατασκευαστή στο σύνολό τους».

182. Ως εκ τούτου, από την αιτιολογική σκέψη 11 προκύπτει ότι σκοπός δεν είναι οι απαιτήσεις του κανονισμού για την κυβερνοανθεκτικότητα να καλύπτουν ολόκληρη την υποδομή ΤΠ ενός οργανισμού, αλλά μόνο τα δομοστοιχεία λογισμικού που επιτρέπουν την εκτέλεση της λύσης επεξεργασίας δεδομένων. Για παράδειγμα, τα εσωτερικά συστήματα που αφορούν τους ανθρώπινους πόρους, τις μισθοδοσίες, τη διαχείριση των σχέσεων με τους πελάτες, τις σωληνώσεις συνεχούς ενοποίησης/συνεχούς παράδοσης (CI/CD), τη διανομή ενημερώσεων ασφαλείας σε περιφερειακές θέσεις του ίδιου του κατασκευαστή, δεν θα πρέπει να θεωρούνται λύσεις εξ αποστάσεως επεξεργασίας δεδομένων. Ομοίως, τα συστήματα που συνδέονται με δραστηριότητες ελέγχου και δοκιμών, όπως οι δοκιμές διείσδυσης, η διερεύνηση απειλών και οι δραστηριότητες κόκκινης ομάδας, δεν εμπίπτουν στο πεδίο εφαρμογής προϊόντος με ψηφιακά στοιχεία, όπως καλύπτεται από τον κανονισμό για την κυβερνοανθεκτικότητα. Είναι σημαντικό να σημειωθεί ότι, ενώ η εφαρμογή αποτελεσματικών και τακτικών δοκιμών και αξιολογήσεων της ασφάλειας του προϊόντος με ψηφιακά στοιχεία αποτελεί ουσιώδη απαίτηση που ορίζεται στο παράρτημα Ι μέρος ΙΙ σημείο 3 του κανονισμού για την κυβερνοανθεκτικότητα, αυτό δεν συνεπάγεται ότι οι εν λόγω δραστηριότητες πρέπει να θεωρούνται λύσεις εξ αποστάσεως επεξεργασίας δεδομένων για το προϊόν με ψηφιακά στοιχεία.

183. Η αιτιολογική σκέψη 12 επικεντρώνεται στις υπηρεσίες υπολογιστικού νέφους και αναλύει τις περιστάσεις υπό τις οποίες οι υπηρεσίες υπολογιστικού νέφους θα μπορούσαν να θεωρηθούν λύσεις εξ αποστάσεως επεξεργασίας δεδομένων. Η αιτιολογική σκέψη καταλήγει υπενθυμίζοντας ότι οι υπηρεσίες υπολογιστικού νέφους και τα μοντέλα υπηρεσιών υπολογιστικού νέφους εμπίπτουν στο πεδίο εφαρμογής της οδηγίας (ΕΕ) 2022/2555 (NIS 2) ([28]), η οποία θεσπίζει απαιτήσεις διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας για τους παρόχους υπηρεσιών υπολογιστικού νέφους. Οι εν λόγω απαιτήσεις προσδιορίζονται περαιτέρω στον εκτελεστικό κανονισμό (ΕΕ) 2024/2690 της Επιτροπής ([29]).

8.1. **Τι θεωρείται λύση εξ αποστάσεως επεξεργασίας δεδομένων για προϊόν με ψηφιακά στοιχεία;**

184. Ως εκ τούτου, ο ορισμός της εξ αποστάσεως επεξεργασίας δεδομένων που θεσπίζεται στο άρθρο 3 σημείο 2) βασίζεται σε τρία στοιχεία: i) αν η επεξεργασία δεδομένων πραγματοποιείται «εξ αποστάσεως»· ii) αν η απουσία της εν λόγω επεξεργασίας δεδομένων θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του· και iii) αν το λογισμικό έχει σχεδιαστεί και αναπτυχθεί από τον κατασκευαστή ή υπό την ευθύνη του. Στα επόμενα τρία υποτμήματα εξετάζεται λεπτομερέστερα καθένα από τα στοιχεία αυτά.

([28]) Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2690 της Επιτροπής, της 17ης Οκτωβρίου 2024, για τη θέσπιση κανόνων εφαρμογής της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης και τους παρόχους υπηρεσιών εμπιστοσύνης (ΕΕ L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Η έννοια «εξ αποστάσεως»*

185. Παρότι η έννοια «εξ αποστάσεως» που αναφέρεται στο άρθρο 3 σημείο 2) είναι χρήσιμη, δεν επαρκεί, ωστόσο, για να προσδιοριστεί αν ένα προϊόν με ψηφιακά στοιχεία περιλαμβάνει λύση εξ αποστάσεως επεξεργασίας δεδομένων. Επιπλέον, δεδομένης της ποικιλίας των λύσεων που ενδέχεται να εμπίπτουν στην έννοια αυτή, δεν είναι δυνατόν να δοθεί εξαντλητικός ορισμός της έννοιας «εξ αποστάσεως». Απαιτείται κατά περίπτωση αξιολόγηση από τον κατασκευαστή.

186. Στην αιτιολογική σκέψη 11 του κανονισμού για την κυβερνοανθεκτικότητα γίνεται αναφορά σε δεδομένα που υποβάλλονται σε επεξεργασία ή αποθηκεύονται «εξ αποστάσεως από τον κατασκευαστή» σε αντίθεση με τα δεδομένα που υποβάλλονται σε επεξεργασία ή αποθηκεύονται «τοπικά στη συσκευή του χρήστη». Η εξ αποστάσεως επεξεργασία δεδομένων πραγματοποιείται συνήθως εκτός του περιβάλλοντος χρήστη προϊόντος με ψηφιακά στοιχεία ή του επιχειρησιακού περιβάλλοντος οργανισμού (για επαγγελματία χρήστη). Ωστόσο, αυτό δεν εμποδίζει την πραγματοποίηση της επεξεργασίας κοντά στη συσκευή («περιφερειακά»). Η διαβίβαση δεδομένων μπορεί να είναι ενσύρματη (π.χ. καλώδιο ethernet) ή ασύρματη (π.χ. Wi-Fi, Bluetooth). Το υπολογιστικό νέφος, συμπεριλαμβανομένης της υπολογιστικής παρυφών, αποτελεί τυπικό παράδειγμα επεξεργασίας δεδομένων που πραγματοποιείται «εξ αποστάσεως». Για παράδειγμα, στην περίπτωση λειτουργίας υπολογιστικού νέφους στην οποία ο χρήστης αποκτά πρόσβαση από εφαρμογή για φορητές συσκευές, μέρος της επεξεργασίας δεδομένων πραγματοποιείται στο υπολογιστικό νέφος, εκτός του περιβάλλοντος του χρήστη.

187. Είναι σημαντικό να σημειωθεί ότι οι λύσεις εξ αποστάσεως επεξεργασίας δεδομένων δεν λειτουργούν κατ' ανάγκη σε υποδομές υπολογιστικού νέφους τρίτων. Η εξ αποστάσεως επεξεργασία δεδομένων που πραγματοποιείται σε τοπικούς διακομιστές στις εγκαταστάσεις του κατασκευαστή μπορεί επίσης να αποτελεί λύση εξ αποστάσεως επεξεργασίας δεδομένων. Με άλλα λόγια, μια λύση που εκτελείται εντός των εγκαταστάσεων και σε ιδιωτικό υπολογιστικό νέφος είναι εξίσου πιθανό να χαρακτηριστεί ως λύση εξ αποστάσεως επεξεργασίας δεδομένων με μια λύση που εκτελείται σε δημόσιο υπολογιστικό νέφος και εκτός των εγκαταστάσεων.

188. Τα δύο καθοριστικά ερωτήματα σωρευτικού χαρακτήρα που καθορίζουν αν η επεξεργασία δεδομένων καλύπτεται από τον κανονισμό για την κυβερνοανθεκτικότητα ως λύση εξ αποστάσεως επεξεργασίας δεδομένων παρατίθενται κατωτέρω, στα τμήματα *8.1.2* και *8.2*. Σε περίπτωση καταφατικής απάντησης και στα δύο ερωτήματα, η εξ αποστάσεως επεξεργασία δεδομένων μπορεί να χαρακτηριστεί ως λύση εξ αποστάσεως επεξεργασίας δεδομένων.

8.1.2. *Η απουσία της εν λόγω επεξεργασίας δεδομένων θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του;*

189. Σύμφωνα με τον ορισμό της «εξ αποστάσεως επεξεργασίας δεδομένων» που περιλαμβάνεται στο άρθρο 3 σημείο 2), για να χαρακτηριστεί η εξ αποστάσεως επεξεργασία δεδομένων ως λύση εξ αποστάσεως επεξεργασίας δεδομένων, η απουσία της θα πρέπει να εμποδίζει το προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του. Η έννοια των «λειτουργιών» που περιλαμβάνεται στον ορισμό αυτόν δεν περιορίζεται στη «βασική λειτουργικότητα» ή στον «επιδιωκόμενο σκοπό» του προϊόντος με ψηφιακά στοιχεία, καθώς ο κανονισμός για την κυβερνοανθεκτικότητα δεν επιβάλλει τέτοιο περιορισμό. Οι λειτουργίες που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα είναι τόσο λειτουργίες που εκπληρώνουν άμεσα τον επιδιωκόμενο σκοπό του προϊόντος με ψηφιακά στοιχεία, όπως τον αντιλαμβάνονται οι χρήστες, όσο και λειτουργίες που υποστηρίζουν τις συνολικές επιδόσεις του προϊόντος.

190. Παραδείγματα λειτουργιών σε σχέση με τις οποίες μπορεί να πραγματοποιηθεί εξ αποστάσεως επεξεργασία δεδομένων και οι οποίες θα εμπόδιζαν ένα προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του θα μπορούσαν να περιλαμβάνουν: i) αποστολή εντολών σε συσκευή· ii) συγχρονισμός αρχείων· iii) ένταξη του χρήστη· iv) διαμόρφωση (εξατομίκευση του προϊόντος με ψηφιακά στοιχεία)· v) αυτοματοποιημένη διανομή ενημερώσεων, συμπεριλαμβανομένης της ενημέρωσης χαρακτηριστικών και των ενημερώσεων ασφαλείας· vi) διαχείριση ταυτότητας και πρόσβασης.

191. Σε ορισμένες περιπτώσεις, ο χρήστης μπορεί να χρησιμοποιεί μια λειτουργία τόσο εξ αποστάσεως όσο και χειροκίνητα (π.χ. χειρισμός λαμπτήρα με εφαρμογή ή χειροκίνητα). Η δυνατότητα αυτή δεν αποκλείει τον χαρακτηρισμό ως λύσης εξ αποστάσεως επεξεργασίας δεδομένων της επεξεργασίας δεδομένων που συνδέεται με την εξ αποστάσεως εκτέλεση της λειτουργίας. Η εξ αποστάσεως εκτέλεση αυτής της λειτουργίας θεωρείται επίσης μέρος των λειτουργιών που προσφέρει το προϊόν με ψηφιακά στοιχεία.

192. Αντιθέτως, όταν η απουσία συγκεκριμένης επεξεργασίας δεδομένων δεν εμποδίζει το προϊόν με ψηφιακά στοιχεία να εκτελεί κάποια από τις λειτουργίες του, η εν λόγω επεξεργασία δεν θεωρείται λύση εξ αποστάσεως επεξεργασίας δεδομένων κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα. Σε αυτό το πλαίσιο περιλαμβάνεται, για παράδειγμα, η εξ αποστάσεως ανάλυση δεδομένων τηλεμετρίας που συλλέγονται αποκλειστικά για στατιστικούς σκοπούς ή για τη μελλοντική ανάπτυξη προϊόντων.

193. Ωστόσο, ακόμα και όταν η επεξεργασία δεδομένων δεν υποστηρίζει μια λειτουργία ενός προϊόντος με ψηφιακά στοιχεία, οι κατασκευαστές ενδέχεται να χρειαστεί να εξετάσουν αν τα εν λόγω εξ αποστάσεως δομοστοιχεία ενέχουν κινδύνους για το προϊόν με ψηφιακά στοιχεία στο πλαίσιο της οικείας εκτίμησης κινδύνων για την κυβερνοασφάλεια (π.χ. υπό το πρίσμα του επιχειρησιακού περιβάλλοντος του προϊόντος) και να μετριάσουν αναλόγως τους εν λόγω κινδύνους (π.χ. μέσω μέτρων μετριασμού σε επίπεδο προϊόντος).

194. Οι ιστότοποι αποτελούν ειδική περίπτωση που χρήζει περαιτέρω διευκρινίσεων, όπως εξηγείται επίσης στο *τμήμα 2.1 Placing on the market*. Οι ιστότοποι δεν εμπίπτουν στο πεδίο εφαρμογής των λύσεων εξ αποστάσεως επεξεργασίας δεδομένων εάν δεν υποστηρίζουν μια λειτουργία προϊόντος με ψηφιακά στοιχεία, όπως εξηγείται στην αιτιολογική σκέψη 11 του κανονισμού για την κυβερνοανθεκτικότητα. Δεν αρκεί ένας ιστότοπος να περιέχει πληροφορίες σχετικά με προϊόν με ψηφιακά στοιχεία για να θεωρηθεί ότι εμπίπτει στο πεδίο εφαρμογής των λύσεων εξ αποστάσεως επεξεργασίας δεδομένων, ακόμα και αν το προϊόν ανακατευθύνει στον εν λόγω ιστότοπο. Για παράδειγμα, η ανακατεύθυνση των χρηστών σε εξωτερική ιστοσελίδα που παρέχει πληροφορίες και οδηγίες στους χρήστες δεν αποτελεί λύση εξ αποστάσεως επεξεργασίας δεδομένων. Αντιθέτως, ένας ιστότοπος μπορεί να εμπίπτει στο πεδίο εφαρμογής των λύσεων εξ αποστάσεως επεξεργασίας δεδομένων εάν καθιστά δυνατή ή υποστηρίζει μια λειτουργία προϊόντος με ψηφιακά στοιχεία. Για παράδειγμα, μια πύλη επαλήθευσης ταυτότητας που εκδίδει διαπιστευτήρια ή αδειοδοτικά που απαιτούνται για τη λειτουργία του προϊόντος με ψηφιακά στοιχεία θα θεωρείται λύση εξ αποστάσεως επεξεργασίας δεδομένων (υπό την προϋπόθεση ότι πληρούνται επίσης τα άλλα κριτήρια του ορισμού).

8.1.3. *Το λογισμικό έχει σχεδιαστεί και αναπτυχθεί από τον κατασκευαστή ή υπό την ευθύνη του;*

195. Στον ορισμό της «εξ αποστάσεως επεξεργασίας δεδομένων» του άρθρου 3 σημείο 2) του κανονισμού για την κυβερνοανθεκτικότητα διευκρινίζεται περαιτέρω ότι το λογισμικό της εν λόγω εξ αποστάσεως επεξεργασίας δεδομένων πρέπει να σχεδιάζεται και να αναπτύσσεται από τον κατασκευαστή ή υπό την ευθύνη του. Η εξ αποστάσεως επεξεργασία δεδομένων που έχει αναπτυχθεί και σχεδιαστεί εξ ολοκλήρου από τον κατασκευαστή (εσωτερικά) είναι φυσικό να χαρακτηριστεί ως λύση εξ αποστάσεως επεξεργασίας δεδομένων. Το ίδιο θα ισχύει αν οι κατασκευαστές βασίζονται σε εξωτερικό πάροχο υπηρεσιών για την ανάπτυξη και τον σχεδιασμό μιας λύσης (δηλαδή «υπό την ευθύνη τους»). Η φράση «υπό την ευθύνη του κατασκευαστή» αναφέρεται σε λύσεις εξ αποστάσεως επεξεργασίας ειδικά προσαρμοσμένες για τον κατασκευαστή. Πρόκειται για περιπτώσεις στις οποίες ο κατασκευαστής δεν χορηγεί απλώς άδεια για υφιστάμενο προϊόν με ψηφιακά στοιχεία ή υπηρεσία το οποίο/την οποία ένας πάροχος υπηρεσιών προσφέρει στους πελάτες του, ή για ελαφρώς τροποποιημένες εκδόσεις αυτών. Η φράση «[Υ]πό την ευθύνη του κατασκευαστή» σημαίνει ότι το λογισμικό κατασκευάζεται αποκλειστικά από τον κατασκευαστή ή για λογαριασμό του, με βάση τα σχέδια και τις προδιαγραφές που αυτός παρέχει.

196. Για την κατανόηση της λύσης εξ αποστάσεως επεξεργασίας δεδομένων, η έννοια του «ποιος διαχειρίζεται τη λύση» δεν αποτελεί καθοριστικό παράγοντα, καθώς ο ορισμός του κανονισμού για την κυβερνοανθεκτικότητα αναφέρεται μόνο στον σχεδιασμό και στην ανάπτυξη της λύσης εξ αποστάσεως επεξεργασίας δεδομένων. Τα παραπάνω συνάδουν με την προσέγγιση του κανονισμού για την κυβερνοανθεκτικότητα, σύμφωνα με την οποία οι απαιτήσεις και οι υποχρεώσεις βαρύνουν τους κατασκευαστές και όχι τη λειτουργία του προϊόντος με ψηφιακά στοιχεία. Εάν οι κατασκευαστές σχεδιάζουν και αναπτύσσουν λύσεις, τις οποίες στη συνέχεια χειρίζονται τρίτοι, παραμένουν υπεύθυνοι για τη συμμόρφωση με τις ουσιώδεις απαιτήσεις του κανονισμού για την κυβερνοανθεκτικότητα για το προϊόν με ψηφιακά στοιχεία που θέτουν σε κυκλοφορία στην αγορά.

197. Είναι αναγκαίο να γίνει διάκριση μεταξύ των περιπτώσεων στις οποίες ο σχεδιασμός και η ανάπτυξη πραγματοποιούνται από τους κατασκευαστές (ή υπό την ευθύνη τους) και των περιπτώσεων εξάρτησης από λύσεις τρίτων που δεν σχεδιάστηκαν και δεν αναπτύχθηκαν από τους κατασκευαστές (ή υπό την ευθύνη τους). Για παράδειγμα, είναι χρήσιμο να εξεταστούν τα συνηθέστερα μοντέλα υπηρεσιών υπολογιστικού νέφους που παρέχουν διαφορετικούς βαθμούς ελέγχου των χρηστών και τα οποία αναφέρονται επίσης στην αιτιολογική σκέψη 12 του κανονισμού για την κυβερνοανθεκτικότητα, δηλαδή το λογισμικό ως υπηρεσία (SaaS), η πλατφόρμα ως υπηρεσία (PaaS) και η υποδομή ως υπηρεσία (IaaS).

198. Στην περίπτωση λύσης IaaS τρίτων, ο κατασκευαστής δεν διαχειρίζεται ούτε ελέγχει τους υποκείμενους υλικούς και εικονικούς πόρους [όπως το υποκείμενο υλισμικό και ο επόπτης (hypervisor) του παρόχου υπηρεσιών υπολογιστικού νέφους], αλλά είναι σε θέση να αναπτύσσει και να εκτελεί οποιοδήποτε λογισμικό χρησιμοποιώντας τους εν λόγω πόρους, όπως λειτουργικά συστήματα και εφαρμογές. Το λογισμικό αυτό σχεδιάζεται και αναπτύσσεται από τον κατασκευαστή ή υπό την ευθύνη του και, ως εκ τούτου, μπορεί να χαρακτηριστεί ως λύση εξ αποστάσεως επεξεργασίας δεδομένων (εφόσον πληροί τα υπόλοιπα στοιχεία του ορισμού).

199. Στην περίπτωση λύσης PaaS τρίτων, ο κατασκευαστής εγκαθιστά τη δική του (δημιουργηθείσα ή αποκτηθείσα) εφαρμογή χρησιμοποιώντας γλώσσες προγραμματισμού και περιβάλλοντα εκτέλεσης που παρέχονται από τον πάροχο υπηρεσιών υπολογιστικού νέφους και ενσωματώνει την εφαρμογή στο προϊόν του με ψηφιακά στοιχεία. Ο κατασκευαστής έχει τον έλεγχο της εφαρμογής και, ενδεχομένως, των ρυθμίσεων διαμόρφωσης για το περιβάλλον εκτέλεσης. Επομένως, η εφαρμογή σχεδιάζεται και αναπτύσσεται από τον κατασκευαστή ή υπό την ευθύνη του και, ως εκ τούτου, μπορεί να χαρακτηριστεί ως λύση εξ αποστάσεως επεξεργασίας δεδομένων (εφόσον πληροί τα υπόλοιπα στοιχεία του ορισμού).

200. Στην περίπτωση λύσης SaaS τρίτων, ο πάροχος SaaS προσφέρει στον κατασκευαστή μια πλήρως αναπτυγμένη εφαρμογή που θα ενσωματωθεί στο προϊόν του κατασκευαστή με ψηφιακά στοιχεία. Ο κατασκευαστής έχει περιορισμένη δυνατότητα να διαχειρίζεται τις ρυθμίσεις διαμόρφωσης της εφαρμογής που αφορούν ειδικά τον χρήστη. Ως εκ τούτου, η εφαρμογή δεν σχεδιάζεται ούτε αναπτύσσεται από τον κατασκευαστή ή υπό την ευθύνη του.

201. Ωστόσο, όταν ορισμένα στοιχεία δεν χαρακτηρίζονται ως λύσεις εξ αποστάσεως επεξεργασίας δεδομένων (π.χ. ο επόπτης στην περίπτωση υποδομής IaaS τρίτων, το λειτουργικό σύστημα στην περίπτωση λύσης PaaS τρίτων ή η εφαρμογή SaaS τρίτων), αλλά ενσωματώνονται στο προϊόν με ψηφιακά στοιχεία με τρόπο που επηρεάζει την ασφάλειά του, οι λύσεις αυτές θα πρέπει να θεωρούνται παρόμοιες με δομοστοιχεία τρίτων. Ο κατασκευαστής υποχρεούται να εντοπίζει και να αξιολογεί τους κινδύνους που συνδέονται με την ενσωμάτωση των εν λόγω στοιχείων και να τους αντιμετωπίζει εφαρμόζοντας τις ουσιώδεις απαιτήσεις στο ίδιο το προϊόν με ψηφιακά στοιχεία. Σε αυτό το πλαίσιο μπορεί, κατά περίπτωση, να υποστηρίζεται από τις λειτουργίες ασφάλειας που διατίθενται από τον πάροχο υπηρεσιών υπολογιστικού νέφους μέσω του μοντέλου επιμερισμένης ευθύνης του, όταν ο κατασκευαστής χρησιμοποιεί ή διαμορφώνει τις εν λόγω λειτουργίες για την αντιμετώπιση των εντοπισθέντων κινδύνων. Επιπλέον, ο κατασκευαστής αναμένεται να εκπληρώνει παρόμοια υποχρέωση με την υποχρέωση επίδειξης δέουσας επιμέλειας που αναφέρεται στο άρθρο 13 παράγραφος 5 σχετικά με την ασφάλεια των εν λόγω δομοστοιχείων, με τρόπο αναλογικό προς τον κίνδυνο που ενέχει η εξ αποστάσεως λύση για την ασφάλεια του προϊόντος με ψηφιακά στοιχεία.

202. Ως εκ τούτου, συνοψίζοντας, προκύπτει ότι:

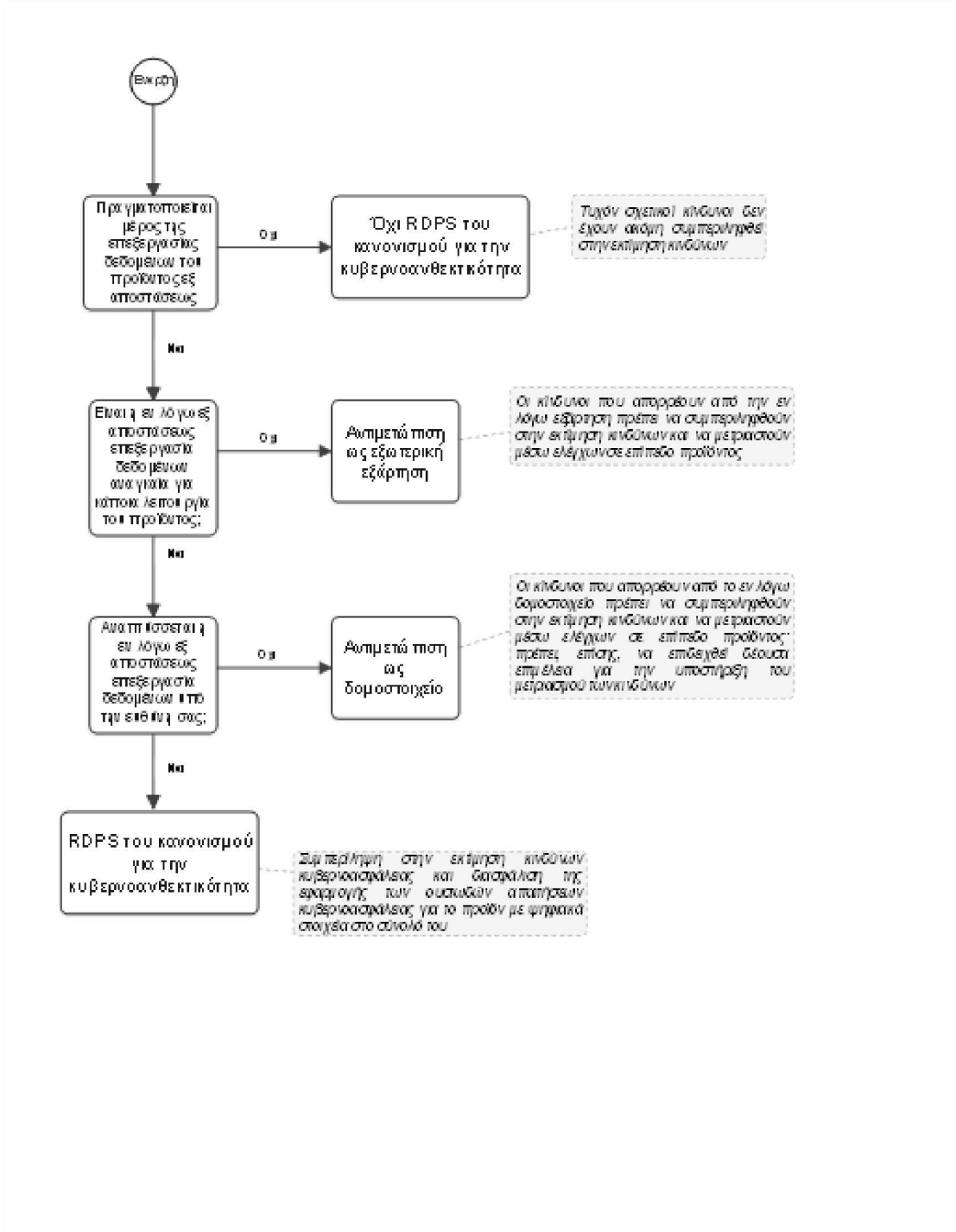
α) Για να χαρακτηριστεί η επεξεργασία δεδομένων ως λύση εξ αποστάσεως επεξεργασίας δεδομένων, η απάντηση και στα δύο ερωτήματα στα τμήματα *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its* functions? και *8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility?* πρέπει να είναι καταφατική.

β) Εάν η απάντηση στο ερώτημα του τμήματος *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its* functions? είναι αρνητική, οι κατασκευαστές θα πρέπει να αξιολογούν τους κινδύνους που απορρέουν από την ύπαρξη της εν λόγω επεξεργασίας δεδομένων στο πλαίσιο της εκτίμησης κινδύνων που διενεργούν.

γ) Εάν η απάντηση στο ερώτημα του τμήματος *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its* functions? είναι καταφατική, αλλά η απάντηση στο ερώτημα του τμήματος *8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility?* είναι αρνητική, οι κατασκευαστές θα πρέπει να αντιμετωπίζουν τη λύση τρίτων ως δομοστοιχείο. Στο πλαίσιο της εκτίμησης κινδύνων, οι κατασκευαστές θα πρέπει να αξιολογούν τους κινδύνους που απορρέουν από την ενσωμάτωση της εν λόγω λύσης και να τους μετριάζουν αναλόγως. Επιπλέον, οι κατασκευαστές θα πρέπει να επιδεικνύουν δέουσα επιμέλεια.

Διάγραμμα 9

Απλοποιημένο διάγραμμα ροής για τον προσδιορισμό του αν ένα προϊόν με ψηφιακά στοιχεία περιλαμβάνει λύσεις εξ αποστάσεως επεξεργασίας δεδομένων



8.2. **Πρακτικές και τεχνικές επιπτώσεις των λύσεων εξ αποστάσεως επεξεργασίας δεδομένων και εξάρτηση από λύσεις τρίτων**

203. Ο κανονισμός για την κυβερνοανθεκτικότητα ακολουθεί προσέγγιση βάσει κινδύνου, η οποία κατοχυρώνεται στο άρθρο 13 παράγραφοι 2 και 3, καθώς και στην πρώτη ουσιώδη απαίτηση του παραρτήματος Ι μέρος Ι, σύμφωνα με την οποία «Τα προϊόντα με ψηφιακά στοιχεία σχεδιάζονται, αναπτύσσονται και παράγονται κατά τρόπο ώστε να εγγυώνται κατάλληλο επίπεδο κυβερνοασφάλειας βάσει των κινδύνων». Κατά συνέπεια, κατά την εφαρμογή των απαιτήσεων του κανονισμού για την κυβερνοανθεκτικότητα στις λύσεις εξ αποστάσεων επεξεργασίας δεδομένων και την αντιμετώπιση των κινδύνων που απορρέουν από υπηρεσίες τρίτων οι οποίες είναι ενσωματωμένες στο προϊόν με ψηφιακά στοιχεία θα πρέπει να λαμβάνεται υπόψη μια προσέγγιση βάσει κινδύνων.

204. Πρώτον, οι κατασκευαστές θα πρέπει i) να αναφέρουν στον τεχνικό φάκελο ότι το προϊόν τους με ψηφιακά στοιχεία περιλαμβάνει λύσεις εξ αποστάσεως επεξεργασίας δεδομένων ή βασίζεται σε εξ αποστάσεως λύσεις τρίτων και ii) να περιγράφουν τις εν λόγω λύσεις. Εάν οι ίδιες λύσεις εξ αποστάσεως επεξεργασίας δεδομένων υποστηρίζουν διάφορα προϊόντα με ψηφιακά στοιχεία, οι λύσεις εξ αποστάσεως επεξεργασίας δεδομένων πρέπει να δηλώνονται στον τεχνικό φάκελο κάθε προϊόντος. Η τεκμηρίωση σχετικά με τις λύσεις εξ αποστάσεως επεξεργασίας δεδομένων που εξυπηρετούν διάφορα προϊόντα με ψηφιακά στοιχεία μπορεί να επαναχρησιμοποιηθεί από την αξιολόγηση της συμμόρφωσης ενός προϊόντος στην αξιολόγηση της συμμόρφωσης άλλου προϊόντος.

205. Όπως αναφέρεται στην αιτιολογική σκέψη 11, οι λύσεις εξ αποστάσεως επεξεργασίας δεδομένων που αποτελούν μέρος του προϊόντος με ψηφιακά στοιχεία και, ως εκ τούτου, υπόκεινται στην αξιολόγηση συμμόρφωσης του προϊόντος θα πρέπει να περιορίζονται στις μονάδες λογισμικού που είναι υπεύθυνες για τη λειτουργικότητα του προϊόντος με ψηφιακά στοιχεία και στις διεπαφές που χρησιμοποιούν οι εν λόγω μονάδες με εξωτερικές υπηρεσίες. Περαιτέρω συστήματα υποστηρικτικών λειτουργιών που πραγματοποιούν μεταγενέστερη επεξεργασία και με τα οποία το προϊόν με ψηφιακά στοιχεία δεν αλληλεπιδρά άμεσα δεν θεωρούνται λύσεις εξ αποστάσεως επεξεργασίας δεδομένων.

206. Ωστόσο, τα εν λόγω συστήματα υποστηρικτικών λειτουργιών παραμένουν εξωτερικές εξαρτήσεις που πρέπει να αξιολογούνται στο πλαίσιο της εκτίμησης κινδύνων για την κυβερνοασφάλεια και να μετριάζονται μέσω μέτρων σε επίπεδο προϊόντος. Στην πραγματικότητα, η εκτίμηση κινδύνων που διενεργείται από τον κατασκευαστή θα πρέπει να λαμβάνει υπόψη: i) τους κινδύνους που σχετίζονται με τις λύσεις εξ αποστάσεως επεξεργασίας δεδομένων· ii) τους κινδύνους που σχετίζονται με την εξάρτηση από εξ αποστάσεως λύσεις τρίτων (παρόμοιες με τα δομοστοιχεία τρίτων)· και iii) τους κινδύνους που σχετίζονται με το περιβάλλον του προϊόντος (π.χ. υποκείμενο υλισμικό). Οι κατασκευαστές θα πρέπει να εφαρμόζουν ελέγχους ασφάλειας στο ίδιο το προϊόν με ψηφιακά στοιχεία για τον μετριασμό των εν λόγω κινδύνων.

207. Επιπλέον, στο πλαίσιο της αξιολόγησης της συμμόρφωσης και/ή της εκπλήρωσης των υποχρεώσεων δέουσας επιμέλειας που σχετίζονται με εξ αποστάσεως υπηρεσίες τρίτων, ο ακόλουθος μη εξαντλητικός κατάλογος τεχνουργημάτων διασφάλισης μπορεί να επαναχρησιμοποιηθεί προς υποστήριξη της αξιολόγησης του κατασκευαστή:

α) αποδεικτικά στοιχεία εκπλήρωσης των υποχρεώσεων που απορρέουν από τον εκτελεστικό κανονισμό (ΕΕ) 2024/2690 της Επιτροπής·

β) αποδεικτικά στοιχεία εκπλήρωσης των υποχρεώσεων που απορρέουν από τον κανονισμό (ΕΕ) 2022/2554 (DORA)·

γ) δήλωση συμμόρφωσης ή πιστοποιητικό που έχει αποκτηθεί στο πλαίσιο ευρωπαϊκού καθεστώτος πιστοποίησης της κυβερνοασφάλειας [που θεσπίστηκε δυνάμει του κανονισμού (ΕΕ) 2019/881 — πράξη για την κυβερνοασφάλεια]·

δ) αποδεικτικά στοιχεία συμμόρφωσης με το πρότυπο ISO/IEC 27017:2015 ή το πρότυπο ISO/IEC 27001:2022.

208. Τέλος, στις αλληλεπιδράσεις τους με τρίτους παρόχους εξ αποστάσεως υπηρεσιών, οι κατασκευαστές πρέπει να εφαρμόζουν τα πλέον κατάλληλα μέτρα ασφάλειας με βάση την εκτίμηση κινδύνων τους (και, κατά περίπτωση, με την υποστήριξη του μοντέλου επιμερισμένης ευθύνης του παρόχου). Τα εν λόγω μέτρα μετριασμού θα πρέπει να περιλαμβάνουν ελέγχους ασφαλείας για τα προϊόντα τους με ψηφιακά στοιχεία και την επαλήθευση των μέτρων ασφαλείας που παρέχονται από τους ίδιους τους τρίτους παρόχους (δέουσα επιμέλεια). Ένα εργαλείο για τον μετριασμό των εν λόγω κινδύνων μπορεί να είναι η ενσωμάτωση εγγυήσεων ασφάλειας στις συμφωνίες επιπέδου υπηρεσιών (ΣΕΥ) που συνάπτουν με τρίτους παρόχους, συμπεριλαμβανομένων διασφαλίσεων ότι οι πάροχοι χειρίζονται επαρκώς τις ευπάθειες. Μια σημαντική αλλαγή στις λύσεις που παρέχονται από τους τρίτους παρόχους εξ αποστάσεως υπηρεσιών δεν θα πρέπει να χαρακτηρίζεται ως ουσιαστική τροποποίηση του προϊόντος με ψηφιακά στοιχεία, καθώς τα στοιχεία αυτά δεν εμπίπτουν στην ευθύνη του κατασκευαστή. Ωστόσο, στο πλαίσιο των υποχρεώσεων δέουσας επιμέλειας που υπέχουν και για τον ορθό μετριασμό των κινδύνων που απορρέουν από τη χρήση τρίτων παρόχων, οι κατασκευαστές ενθαρρύνονται να διασφαλίζουν ότι οι τρίτοι πάροχοι υπηρεσιών υπολογιστικού νέφους τούς τηρούν επαρκώς ενήμερους σχετικά με τις αλλαγές που εφαρμόζουν στις λύσεις τους. Με βάση τις πληροφορίες αυτές, οι κατασκευαστές ενδέχεται να χρειαστεί να αναθεωρήσουν την εκτίμηση κινδύνων που διενεργούν. Στην επικαιροποιημένη εκτίμηση κινδύνων θα πρέπει να εξετάζεται το αν οι τρίτοι πάροχοι υπηρεσιών εξακολουθούν να παρέχουν επαρκείς εγγυήσεις όσον αφορά την κυβερνοασφάλεια και αν οι έλεγχοι ασφάλειας σε επίπεδο προϊόντος εξακολουθούν να είναι επαρκείς. Σε ορισμένες περιπτώσεις, οι κατασκευαστές ενδέχεται να χρειαστεί να τροποποιήσουν τους εν λόγω ελέγχους ή να αλλάξουν τρίτους παρόχους υπηρεσιών.

8.3. **Περιπτώσεις χρήσης για λύσεις εξ αποστάσεως επεξεργασίας δεδομένων**

Προκειμένου να παρασχεθεί πρόσθετη πρακτική καθοδήγηση στους κατασκευαστές, στο παρόν τμήμα παρατίθεται σειρά υποθετικών περιπτώσεων χρήσης, στις οποίες περιγράφονται αντιπροσωπευτικά προϊόντα με ψηφιακά στοιχεία που βασίζονται στην εξ αποστάσεως επεξεργασία δεδομένων και καταδεικνύεται το αν η εν λόγω επεξεργασία μπορεί να χαρακτηριστεί ως λύση εξ αποστάσεως επεξεργασίας δεδομένων κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα.

8.3.1. *Εφαρμογή κινητής τραπεζικής*

Χρηματοπιστωτική οντότητα θέτει σε κυκλοφορία στην αγορά εφαρμογή κινητής τραπεζικής. Τα συστήματα υποστηρικτικών λειτουργιών της εφαρμογής υποστηρίζουν, μεταξύ άλλων, την επαλήθευση ταυτότητας, την έγκριση, τη διαχείριση λογαριασμών και τις πληρωμές. Η χρηματοπιστωτική οντότητα χρησιμοποιεί υβριδική στρατηγική που βασίζεται σε εσωτερικές υποδομές, καθώς και σε εξ αποστάσεως λύσεις τρίτων για την υποστήριξη των λειτουργιών της εφαρμογής. Σε αυτές περιλαμβάνονται οι εξής:

Αυτοφιλοξενούμενη υποδομή που έχει αναπτυχθεί από τη χρηματοπιστωτική οντότητα:

— Ο πελάτης ανοίγει την εφαρμογή κινητής τραπεζικής και επαληθεύεται η ταυτότητά του μέσω της διεπαφής τραπεζικής, μιας αυτοφιλοξενούμενης λύσης που αναπτύχθηκε από τη χρηματοπιστωτική οντότητα, η οποία λαμβάνει τα αιτήματα της εφαρμογής και επιστρέφει τις αντίστοιχες απαντήσεις. Η διεπαφή τραπεζικής επαληθεύει την ταυτότητα του πελάτη πραγματοποιώντας αναζήτηση στο σύστημα διαχείρισης λογαριασμών και παρέχει πρόσβαση στην εφαρμογή.

— Ο πελάτης δίνει εντολή μεταφοράς μέσω της εφαρμογής. Η εφαρμογή διαβιβάζει την εντολή στη διεπαφή τραπεζικής, η οποία υποβάλει αντίστοιχο αίτημα στο σύστημα καθολικού.

— Το σύστημα διαχείρισης λογαριασμών και το σύστημα καθολικού, τα οποία είναι αυτοφιλοξενούμενα αλλά διαχωρίζονται λογικά από τη διεπαφή τραπεζικής, καταγράφουν τη συναλλαγή.

— Το σύστημα καθολικού επιστρέφει την κατάσταση της συναλλαγής στη διεπαφή τραπεζικής, η οποία παρουσιάζει το αποτέλεσμα στον πελάτη.

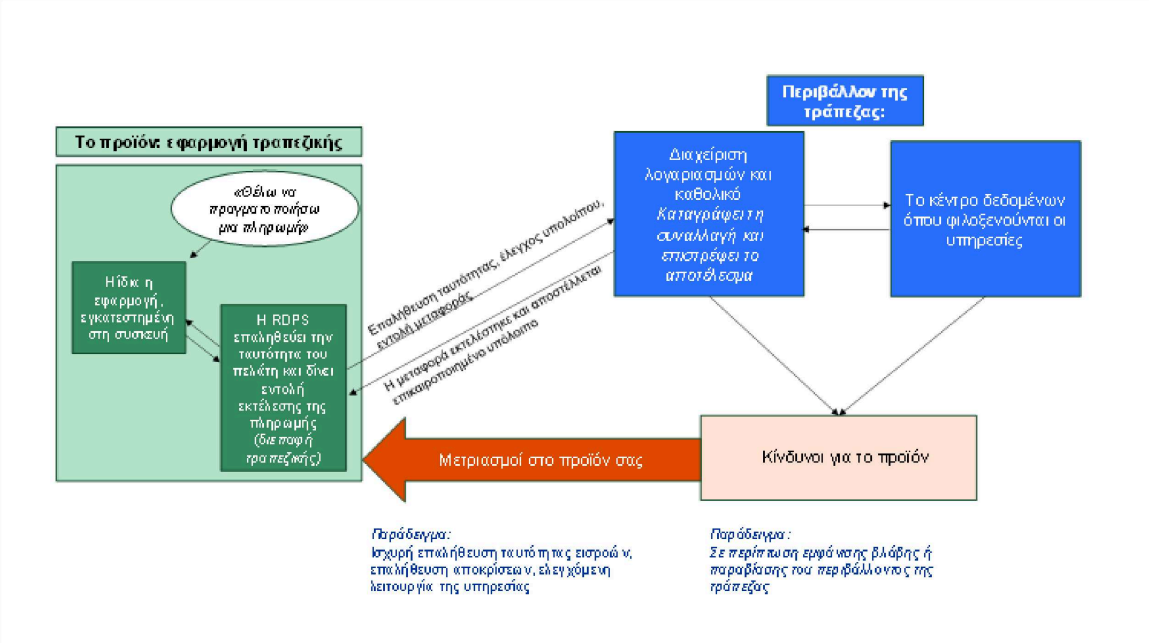
Επιπτώσεις για τις λύσεις εξ αποστάσεως επεξεργασίας δεδομένων:

— Η διεπαφή τραπεζικής είναι απαραίτητη για την εκτέλεση των λειτουργιών της εφαρμογής, δηλαδή την επαλήθευση της ταυτότητας του πελάτη, την υποβολή των εντολών του πελάτη, συμπεριλαμβανομένων των εντολών πληρωμής και μεταφοράς και την εμφάνιση της κατάστασης που προκύπτει. Η διεπαφή τραπεζικής σχεδιάζεται και αναπτύσσεται υπό την ευθύνη του κατασκευαστή. Δεδομένου ότι η απάντηση και στα δύο ερωτήματα που παρουσιάστηκαν στα προηγούμενα τμήματα είναι καταφατική, η διεπαφή τραπεζικής πρέπει να θεωρηθεί λύση εξ αποστάσεως επεξεργασίας δεδομένων. Ως εκ τούτου, πρέπει να περιληφθεί στην εκτίμηση κινδύνων για την κυβερνοασφάλεια και στην εφαρμογή των ουσιωδών απαιτήσεων για το προϊόν με ψηφιακά στοιχεία στο σύνολό του. Η μεταγενέστερη επεξεργασία εντολής μετά την υποβολή της, ιδίως η καταγραφή της συναλλαγής στα συστήματα διαχείρισης λογαριασμών και καθολικού, ο διακανονισμός και ο συμψηφισμός, πραγματοποιείται από συστήματα με τα οποία η εφαρμογή δεν αλληλεπιδρά άμεσα και, ως εκ τούτου, δεν αποτελεί λύση εξ αποστάσεως επεξεργασίας δεδομένων.

— Το σύστημα διαχείρισης λογαριασμών και το σύστημα καθολικού δεν μπορούν να χαρακτηριστούν λύση εξ αποστάσεως επεξεργασίας δεδομένων για την εφαρμογή τραπεζικής. Η εφαρμογή δεν αλληλεπιδρά άμεσα με αυτά (αντιθέτως, αλληλεπιδρά με τη διεπαφή τραπεζικής, η οποία με τη σειρά της βασίζεται σε αυτά). Μολονότι η διαθεσιμότητά τους μπορεί να είναι αναγκαία για την ολοκλήρωση μιας λειτουργίας, ο κανονισμός για την κυβερνοανθεκτικότητα καλύπτει μόνο τα μέρη του συστήματος που αλληλεπιδρούν άμεσα με το προϊόν με ψηφιακά στοιχεία. Ως εκ τούτου, δεν εμπίπτουν στον ορισμό των λύσεων εξ αποστάσεως επεξεργασίας δεδομένων για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα. Ωστόσο, τα εν λόγω συστήματα παραμένουν εξωτερικές εξαρτήσεις που ενδέχεται να προκαλέσουν σημαντικούς κινδύνους κυβερνοασφάλειας για το προϊόν με ψηφιακά στοιχεία. Για παράδειγμα, η παραβίαση του συστήματος καθολικού θα μπορούσε να επιτρέψει σε έναν επιτιθέμενο να επηρεάσει τα αποτελέσματα των συναλλαγών που εμφανίζονται στη συνέχεια στην εφαρμογή. Ως εκ τούτου, ο κατασκευαστής υποχρεούται να εντοπίζει και να αξιολογεί τους εν λόγω κινδύνους στο πλαίσιο της εκτίμησης κινδύνων για την κυβερνοασφάλεια και να τους μετριάζει μέσω μέτρων σε επίπεδο προϊόντος, όπως η αυστηρή επαλήθευση ταυτότητας των διεπαφών υποστηρικτικών λειτουργιών, η προστασία της ακεραιότητας των δεδομένων συναλλαγών, οι ασφαλείς δίαυλοι επικοινωνίας και η επαλήθευση των αποκρίσεων που λαμβάνει η εφαρμογή.

Διάγραμμα 10

Απλοποιημένη αναπαράσταση εφαρμογής τραπεζικής που βασίζεται σε λύσεις εξ αποστάσεως επεξεργασίας δεδομένων



Λογισμικό ως υπηρεσία (SaaS) τρίτων για υποστήριξη πελατών:

— Η χρηματοπιστωτική οντότητα ενσωματώνει στην εφαρμογή της λύση συνομιλίας υποστήριξης πελατών την οποία αναπτύσσει και διαχειρίζεται τρίτος πάροχος· ο τρίτος πάροχος έχει αναπτύξει τον κώδικα διακομιστή συνομιλίας, έχει κατασκευάσει τη διεπαφή χρήστη και διαχειρίζεται την υποδομή όπου χρησιμοποιείται η συνομιλία (δηλαδή το μοντέλο SaaS).

— Όταν ο πελάτης υποβάλλει αίτημα υποστήριξης, η εφαρμογή συνδέει τον πελάτη με την υπηρεσία τρίτου για τη δημιουργία περιόδου συνομιλίας και τη διαχείριση της ροής μηνυμάτων, χωρίς να παρέχει στον τρίτο πρόσβαση στα βασικά συστήματα τραπεζικής.

Επιπτώσεις για τις λύσεις εξ αποστάσεως επεξεργασίας δεδομένων:

— Η λύση συνομιλίας υποστήριξης είναι απαραίτητη προκειμένου το προϊόν με ψηφιακά στοιχεία να εκτελεί κάποια από τις λειτουργίες του, αλλά δεν έχει σχεδιαστεί ούτε έχει αναπτυχθεί από τη χρηματοπιστωτική οντότητα ή υπό την ευθύνη της· ως εκ τούτου, δεν αποτελεί λύση εξ αποστάσεως επεξεργασίας δεδομένων. Ωστόσο, θα πρέπει να αντιμετωπίζεται ως δομοστοιχείο τρίτου. Η εξάρτηση από την εν λόγω υπηρεσία τρίτου μπορεί να δημιουργήσει κινδύνους κυβερνοασφάλειας για την εφαρμογή τραπεζικής, για παράδειγμα εάν ένας επιτιθέμενος χρησιμοποιήσει τον διαυλο συνομιλίας για να προβεί σε πλαστοπροσωπία τραπεζικών υπαλλήλων ή να διανείμει κακόβουλο περιεχόμενο στους χρήστες. Η χρηματοπιστωτική οντότητα πρέπει να λαμβάνει υπόψη τους εν λόγω κινδύνους στην εκτίμηση κινδύνων για την κυβερνοασφάλεια και να τους μετριάζει μέσω μέτρων σε επίπεδο προϊόντος, όπως η απομόνωση της λειτουργίας συνομιλίας από βασικές λειτουργίες τραπεζικής, ο έλεγχος των ροών δεδομένων και η επικύρωση περιεχομένου. Θα πρέπει επίσης να ασκείται δέουσα επιμέλεια όσον αφορά το λογισμικό ως υπηρεσία (SaaS).

8.3.2. *Έξυπνος θερμοστάτης*

Έξυπνος θερμοστάτης επιτρέπει στους χρήστες να ελέγχουν τη θερμοκρασία του σπιτιού τους μέσω εφαρμογής για φορητές συσκευές. Η εφαρμογή για φορητές συσκευές και ο έξυπνος θερμοστάτης βασίζονται στην εξ αποστάσεως επεξεργασία δεδομένων για την ανταλλαγή δεδομένων (π.χ. αίτημα αύξησης της θερμοκρασίας) και την αποθήκευση δεδομένων (π.χ. προτιμήσεις χρήστη). Οι λειτουργίες αυτές αναπτύχθηκαν και σχεδιάστηκαν υπό την ευθύνη του κατασκευαστή, αλλά εκτελούνται σε υποκείμενη φυσική και εικονική υποδομή που παρέχεται από τρίτους [υποδομή ως υπηρεσία (IaaS) τρίτων].

Δεδομένου ότι ο έξυπνος θερμοστάτης δεν θα μπορούσε να εκτελεί τις έξυπνες λειτουργίες του χωρίς αυτήν την εξ αποστάσεως επεξεργασία δεδομένων, η απουσία της θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελεί μία ή περισσότερες από τις λειτουργίες του. Επιπλέον, το λογισμικό αναπτύχθηκε και σχεδιάστηκε υπό την ευθύνη του κατασκευαστή έξυπνων θερμοστατών. Ως εκ τούτου, η εξ αποστάσεως επεξεργασία δεδομένων μπορεί να χαρακτηριστεί ως λύση εξ αποστάσεως επεξεργασίας δεδομένων, όπως ορίζεται στον κανονισμό για την κυβερνοανθεκτικότητα.

Για τους σκοπούς της συμμόρφωσης με τον κανονισμό για την κυβερνοανθεκτικότητα, ο κατασκευαστής του έξυπνου θερμοστάτη πρέπει να τεκμηριώνει τη λύση εξ αποστάσεως επεξεργασίας δεδομένων, καθώς και την εξάρτηση από την υποδομή ως υπηρεσία (IaaS) τρίτων στον τεχνικό φάκελο του προϊόντος με ψηφιακά στοιχεία, συμπεριλαμβανομένων λεπτομερειών της υπηρεσίας που αποτελεί αντικείμενο της σύμβασης. Ο κατασκευαστής πρέπει να λαμβάνει υπόψη τα εν λόγω στοιχεία στην εκτίμηση κινδύνων, η οποία περιλαμβάνει τον επιδιωκόμενο σκοπό και την ευλόγως προβλέψιμη χρήση του προϊόντος με ψηφιακά στοιχεία. Ο κατασκευαστής εφαρμόζει τις ουσιώδεις απαιτήσεις του κανονισμού για την κυβερνοανθεκτικότητα με βάση τους κινδύνους της λύσης εξ αποστάσεως επεξεργασίας δεδομένων. Για την υποδομή ως υπηρεσία (IaaS) τρίτων, ο κατασκευαστής πρέπει να διασφαλίζει ότι τα μέτρα ασφαλείας που παρέχονται από τον τρίτο πάροχο είναι κατάλληλα και/ή να λαμβάνει σχετικά μέτρα έναντι της υποδομής. Όσον αφορά το πρώτο, ο κατασκευαστής μπορεί, για παράδειγμα, να ζητήσει αποδεικτικά στοιχεία ότι έχουν τηρηθεί οι υποχρεώσεις της οδηγίας NIS 2.

8.3.3. *Συσκευή ανάγνωσης ηλεκτρονικών βιβλίων*

Ο κατασκευαστής λογισμικού συσκευής ανάγνωσης ηλεκτρονικών βιβλίων χρησιμοποιεί υπηρεσία αποθήκευσης με λογισμικό ως υπηρεσία (SaaS) τρίτων για να αποθηκεύει ηλεκτρονικά βιβλία που αγοράζουν οι πελάτες και να τους παρέχει τη δυνατότητα πρόσβασης στα βιβλία τους. Η απουσία αυτής της υπηρεσίας αποθήκευσης θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του, αλλά η υπηρεσία αποθήκευσης με λογισμικό ως υπηρεσία (SaaS) δεν αναπτύσσεται από τον κατασκευαστή ή υπό την ευθύνη του· ο πάροχος λογισμικού ως υπηρεσίας (SaaS) το θέτει στη διάθεση των πελατών για κάθε περίπτωση χρήσης.

Η υπηρεσία αποθήκευσης με λογισμικό ως υπηρεσία (SaaS) δεν πληροί τον ορισμό της λύσης εξ αποστάσεως επεξεργασίας δεδομένων. Ωστόσο, ο κατασκευαστής συσκευών ανάγνωσης ηλεκτρονικών βιβλίων βασίζεται στην εν λόγω εξωτερική υπηρεσία για τη λειτουργία του προϊόντος του με ψηφιακά στοιχεία και, ως εκ τούτου, πρέπει να λαμβάνει υπόψη τους σχετικούς κινδύνους στο πλαίσιο της εκτίμησης κινδύνων για την κυβερνοασφάλεια. Ο κατασκευαστής συσκευών ανάγνωσης ηλεκτρονικών βιβλίων θα πρέπει να αντιμετωπίζει το λογισμικό ως υπηρεσία (SaaS) ως δομοστοιχείο. Ο κατασκευαστής πρέπει να εφαρμόζει κατάλληλα μέτρα ασφάλειας σε επίπεδο προϊόντος, όπως ασφαλή επαλήθευση ταυτότητας, κρυπτογράφηση και προστασία της ακεραιότητας των επικοινωνιών με την υπηρεσία αποθήκευσης. Η επίδειξη δέουσας επιμέλειας κατά την επιλογή και την ενσωμάτωση του παρόχου λογισμικού ως υπηρεσίας (SaaS) θα υποστηρίξει επίσης τις υποχρεώσεις του κατασκευαστή, ώστε το προϊόν με ψηφιακά στοιχεία στο σύνολό του να μπορεί να συμμορφώνεται με τις ουσιώδεις απαιτήσεις.

8.3.4. *Βιομηχανικό ρομπότ*

Ένα βιομηχανικό ρομπότ έχει ως αποστολή να συλλέγει εξαρτήματα. Το ρομπότ αποστέλλει πληροφορίες που συλλέγονται μέσω καμερών σε εξ αποστάσεως υπηρεσία που έχει σχεδιαστεί και αναπτυχθεί από τον κατασκευαστή. Η υπηρεσία αυτή εκτελείται σε υποκείμενη φυσική και εικονική υποδομή που παρέχεται από τρίτο πάροχο υπηρεσιών [υποδομή ως υπηρεσία (IaaS) τρίτων]. Η υπηρεσία υπολογιστικού νέφους υπολογίζει τη θέση ενός εξαρτήματος με βάση τη ροή εικόνας της κάμερας και αποστέλλει εντολές στο ρομπότ για να συλλέξει τα εξαρτήματα.

Η απουσία αυτής της επεξεργασίας δεδομένων θα εμπόδιζε το βιομηχανικό ρομπότ να συλλέξει εξαρτήματα και, ως εκ τούτου, να εκτελέσει κάποια από τις λειτουργίες του. Επιπλέον, το λογισμικό που λειτουργεί επί της υποδομής έχει σχεδιαστεί και αναπτυχθεί από τον κατασκευαστή. Το λογισμικό που σχεδιάστηκε και αναπτύχθηκε από τον κατασκευαστή πληροί τον ορισμό της λύσης εξ αποστάσεως επεξεργασίας δεδομένων.

Ο κατασκευαστής του βιομηχανικού ρομπότ πρέπει να τεκμηριώνει τη λύση εξ αποστάσεως επεξεργασίας δεδομένων, καθώς και την εξάρτηση από την υποδομή ως υπηρεσία (IaaS) τρίτων στον τεχνικό φάκελο του προϊόντος με ψηφιακά στοιχεία (συμπεριλαμβανομένων λεπτομερειών της υπηρεσίας που αποτελεί αντικείμενο της σύμβασης). Ο κατασκευαστής πρέπει επίσης να λαμβάνει υπόψη τα εν λόγω στοιχεία στην εκτίμηση κινδύνων, η οποία περιλαμβάνει τον επιδιωκόμενο σκοπό και την ευλόγως προβλέψιμη χρήση του προϊόντος με ψηφιακά στοιχεία. Ο κατασκευαστής εφαρμόζει τις ουσιώδεις απαιτήσεις του κανονισμού για την κυβερνοανθεκτικότητα για το προϊόν με ψηφιακά στοιχεία, συμπεριλαμβανομένων των οικείων λύσεων εξ αποστάσεως επεξεργασίας δεδομένων, με βάση τους κινδύνους. Η δέουσα επιμέλεια κατά την επιλογή του παρόχου υποδομής ως υπηρεσίας (IaaS) θα υποστηρίξει επίσης τις υποχρεώσεις του κατασκευαστή. Για παράδειγμα, ο κατασκευαστής θα μπορούσε να ζητήσει αποδεικτικά στοιχεία ότι έχουν εκπληρωθεί οι υποχρεώσεις της οδηγίας NIS 2.

8.3.5. *Κυψελοειδές δίκτυο*

Έξυπνο τηλέφωνο βασίζεται σε δίκτυο 5G για την παροχή σύνδεσης στο διαδίκτυο, τηλεφωνικών κλήσεων και μηνυμάτων στους χρήστες του (κινητή συνδεσιμότητα). Το κυψελοειδές δίκτυο αναπτύσσεται και σχεδιάζεται από φορείς εκμετάλλευσης τηλεπικοινωνιών. Το δίκτυο περιλαμβάνει μικρές κυψέλες και πύργους κινητής τηλεφωνίας, καθώς και άλλο εξοπλισμό δικτύου.

Το προϊόν με ψηφιακά στοιχεία θα πρέπει να μπορεί να συνδέεται ορθά με ένα δίκτυο· αυτή είναι μία από τις λειτουργίες του. Ωστόσο, το αν το εν λόγω δίκτυο λειτουργεί ή όχι δεν έχει σημασία για να εξακριβωθεί αν το προϊόν με ψηφιακά στοιχεία λειτουργεί σωστά. Το δίκτυο αποτελεί μόνο δίαυλο επικοινωνίας και δεν είναι απαραίτητο για την εκτέλεση της λειτουργίας «ορθής σύνδεσης με δίκτυο» του προϊόντος με ψηφιακά στοιχεία. Ομοίως, ένα καλώδιο ethernet, ένας δρομολογητής ή ένα σήμα Wi-Fi δεν θεωρούνται επεξεργασία δεδομένων, η απουσία της οποίας θα εμπόδιζε το προϊόν με ψηφιακά στοιχεία να εκτελέσει κάποια από τις λειτουργίες του, αλλά μάλλον μέσα διευκόλυνσης της επικοινωνίας/συνδεσιμότητας.

Κατά συνέπεια, το κυψελοειδές δίκτυο δεν πληροί τον ορισμό της λύσης εξ αποστάσεως επεξεργασίας δεδομένων. Το δίκτυο δεν θα πρέπει να θεωρείται δομοστοιχείο τρίτων, καθώς δεν υπάρχει λογισμικό ενσωματωμένο στο προϊόν με ψηφιακά στοιχεία, αλλά το προϊόν βασίζεται απλώς σε αυτό το δίκτυο. Ως εκ τούτου, δεν είναι αναγκαίο ο κατασκευαστής να εκπληρώνει υποχρεώσεις επίδειξης δέουσας επιμέλειας έναντι του παρόχου δικτύου.

9. **ΠΡΟΣΘΕΤΑ ΣΤΟΙΧΕΙΑ**

9.1. **Υποχρεώσεις αναφοράς**

209. Σύμφωνα με το άρθρο 14 παράγραφοι 1 και 3 του κανονισμού για την κυβερνοανθεκτικότητα, ο κατασκευαστής υποχρεούται να κοινοποιεί ταυτόχρονα στην ΟΑΠΑΥ στην οποία έχουν ανατεθεί καθήκοντα συντονισμού και στον ENISA i) κάθε ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και περιέχεται στο προϊόν του με ψηφιακά στοιχεία και η οποία υποπίπτει στην αντίληψή του· και ii) κάθε σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία και το οποίο υποπίπτει στην αντίληψή του.

210. Σύμφωνα με το άρθρο 69 παράγραφος 3 και το άρθρο 71 παράγραφος 2 δεύτερη περίοδος, η υποχρέωση συμμόρφωσης με το άρθρο 14 εφαρμόζεται από τις 11 Σεπτεμβρίου 2026 σε όλα τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, συμπεριλαμβανομένων των προϊόντων με ψηφιακά στοιχεία που έχουν τεθεί σε κυκλοφορία στην αγορά πριν από τις 11 Δεκεμβρίου 2027. Επιπλέον, σε αντίθεση με τις υποχρεώσεις χειρισμού ευπαθειών, οι οποίες εξακολουθούν να ισχύουν μόνο για τη διάρκεια της περιόδου υποστήριξης ενός προϊόντος, οι υποχρεώσεις αναφοράς εξακολουθούν να ισχύουν και μετά τη λήξη της περιόδου υποστήριξης ενός προϊόντος. Όταν ένα προϊόν με ψηφιακά στοιχεία τέθηκε σε κυκλοφορία στην αγορά πριν από τις 11 Δεκεμβρίου 2027 ή όταν η περίοδος υποστήριξής του έχει λήξει, ο κατασκευαστής δεν απαιτείται να συμμορφώνεται με τις υποχρεώσεις χειρισμού ευπαθειών που ορίζονται στο παράρτημα I μέρος II.

211. Υπενθυμίζεται ότι η υποχρέωση κοινοποίησης τέτοιων συμβάντων ισχύει μόλις υποπέσει στην αντίληψη του κατασκευαστή ότι μια ευπάθεια αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή ότι έχει λάβει χώρα σοβαρό περιστατικό που έχει θέσει σε κίνδυνο την ασφάλεια του προϊόντος του με ψηφιακά στοιχεία. Ως εκ τούτου, η καθοδήγηση σχετικά με το πότε ένα περιστατικό θεωρείται ότι έχει υποπέσει στην αντίληψη κατασκευαστή αναμένεται να βοηθήσει τους κατασκευαστές να προσδιορίζουν τη στιγμή έναρξης των ισχυουσών προθεσμιών αναφοράς.

212. Οι κατασκευαστές ενδέχεται να υπόκεινται σε συγκρίσιμες υποχρεώσεις αναφοράς βάσει διαφόρων πράξεων της ΕΕ. Για να διασφαλιστεί ότι η έννοια του «υποπίπτει στην αντίληψη» ερμηνεύεται με συνέπεια και για να διευκολυνθεί η συμμόρφωση των κατασκευαστών με τις εν λόγω υποχρεώσεις, η παρούσα καθοδήγηση συνάδει με την αιτιολογική σκέψη 31 του εκτελεστικού κανονισμού (ΕΕ) 2024/2690 της Επιτροπής και με την ενότητα II.Α των κατευθυντήριων γραμμών 9/2022 σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του ΓΚΠΔ.

213. Σε ορισμένες περιπτώσεις, ένας κατασκευαστής εντοπίζει ύποπτο συμβάν ή ένα τρίτο μέρος, όπως ένα άτομο, ένας πελάτης, μια οντότητα, μια αρχή, ένας οργανισμός μέσων ενημέρωσης ή άλλη πηγή, εφιστά την προσοχή του σε πιθανό περιστατικό ή ευπάθεια. Στις περιπτώσεις αυτές, ο κατασκευαστής θα πρέπει να αξιολογεί αμέσως το ύποπτο συμβάν για να διαπιστώσει αν συνιστά ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή σοβαρό περιστατικό που έχει αντίκτυπο στην ασφάλεια του προϊόντος με ψηφιακά στοιχεία. Ως εκ τούτου, ο κατασκευαστής πρέπει να θεωρείται ότι έχει λάβει γνώση όταν, μετά από μια τέτοια αρχική αξιολόγηση, έχει εύλογο βαθμό βεβαιότητας ότι: i) μια ευπάθεια που περιέχεται στο προϊόν του με ψηφιακά στοιχεία αποτελεί αντικείμενο ενεργού εκμετάλλευσης· ή ii) έχει λάβει χώρα σοβαρό περιστατικό το οποίο έχει θέσει σε κίνδυνο την ασφάλεια του προϊόντος του με ψηφιακά στοιχεία.

214. Ως εκ τούτου, η χρονική στιγμή κατά την οποία μπορεί να θεωρηθεί ότι ο κατασκευαστής έχει λάβει γνώση θα εξαρτάται από τις περιστάσεις της συγκεκριμένης ευπάθειας που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή του σοβαρού περιστατικού. Σε ορισμένες περιπτώσεις, θα είναι σχετικά σαφές εξαρχής ότι μια ευπάθεια αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή ότι ένα σοβαρό περιστατικό επηρεάζει την ασφάλεια ενός προϊόντος με ψηφιακά στοιχεία. Σε άλλες περιπτώσεις, μπορεί να χρειαστεί κάποιος χρόνος για να διαπιστωθεί αν ένα προϊόν με ψηφιακά στοιχεία επηρεάζεται από ευπάθεια και αν η εν λόγω ευπάθεια αποτελεί αντικείμενο εκμετάλλευσης από κακόβουλο παράγοντα ή αν ένα περιστατικό επηρεάζει την ασφάλεια ενός προϊόντος με ψηφιακά στοιχεία. Ωστόσο, θα πρέπει να δοθεί έμφαση στην ανάληψη άμεσης δράσης για τη διενέργεια της αρχικής αξιολόγησης προκειμένου να διαπιστωθεί αν πληρούνται πράγματι οι εν λόγω προϋποθέσεις, ιδίως όταν η ευπάθεια μπορεί να ενέχει σημαντικό κίνδυνο, και, εάν ναι, να ληφθούν διορθωτικά μέτρα και να πραγματοποιηθεί γνωστοποίηση σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα.

215. Επιπλέον, η δομή των υποχρεώσεων αναφοράς απαιτεί από τους κατασκευαστές να επικαιροποιούν σταδιακά τις κοινοποιήσεις τους, καθώς εξελίσσονται οι εσωτερικές έρευνές τους και καθώς αποκτούν λεπτομερέστερες γνώσεις σχετικά με την ευπάθεια ή το συμβάν που αποτελεί αντικείμενο ενεργού εκμετάλλευσης. Ειδικότερα, οι κατασκευαστές υποχρεούνται να υποβάλλουν κοινοποίηση έγκαιρης προειδοποίησης που περιέχει περιορισμένες πληροφορίες χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που λαμβάνουν γνώση. Στη συνέχεια, απαιτούνται πρόσθετες πληροφορίες στο πλαίσιο της κοινοποίησης, οι οποίες πρέπει να υποβάλλονται χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που λαμβάνουν γνώση (στο εξής: 72ωρη κοινοποίηση). Η πλήρης έκθεση πρέπει να υποβάλλεται εντός 14 ημερών μετά τη λήψη διορθωτικού μέτρου ή μέτρου μετριασμού για ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης ή εντός ενός μηνός από την 72ωρη κοινοποίηση σοβαρών περιστατικών.

216. Όπως υπενθυμίζεται επίσης στο τμήμα *3.3.1 Sustained support and ensuring viability of FOSS*, οι υποστηρικτές λογισμικού ανοικτού κώδικα υποχρεούνται επίσης να αναφέρουν τις ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης σύμφωνα με το άρθρο 24 παράγραφος 3 ([30]). Η υποχρέωση αυτή ισχύει από τη στιγμή που υποπίπτει στην αντίληψη οντότητας ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και όχι μόνο όταν υπάρχει ευπάθεια στη βάση κώδικα ελεύθερου λογισμικού ανοικτού κώδικα του οποίου η εν λόγω οντότητα είναι υποστηρικτής. Στην πράξη, επειδή τα δομοστοιχεία του ελεύθερου λογισμικού ανοικτού κώδικα ενσωματώνονται συνήθως κατάντη σε άλλα προϊόντα με ψηφιακά στοιχεία, ένας υποστηρικτής είναι πιθανό να αντιληφθεί την ενεργό εκμετάλλευση μέσω αναφορών τρίτων, στις οποίες η εκμετάλλευση σε δομοστοιχεία ελεύθερου λογισμικού ανοικτού κώδικα προσδιορίζεται ως ενσωματωμένη σε άλλα προϊόντα με ψηφιακά στοιχεία. Αυτό μπορεί να συμβαίνει, για παράδειγμα, όταν ο κατασκευαστής προϊόντος με ψηφιακά στοιχεία εντοπίζει την ενεργό εκμετάλλευση δομοστοιχείου ελεύθερου λογισμικού ανοικτού κώδικα που είναι ενσωματωμένο στο δικό του προϊόν και την αναφέρει στον υποστηρικτή του εν λόγω δομοστοιχείου· ή όταν ένας χρήστης ή ένας ερευνητής στον τομέα της ασφάλειας εντοπίζει αποδεικτικά στοιχεία εκμετάλλευσης δομοστοιχείου ελεύθερου λογισμικού ανοικτού κώδικα ενσωματωμένου σε προϊόν με ψηφιακά στοιχεία και αναφέρει την εν λόγω ενεργό εκμετάλλευση στον υποστηρικτή του δομοστοιχείου.

217. Θα πρέπει επίσης να διευκρινιστεί ότι, επειδή η υποχρέωση αναφοράς ευπαθειών που αποτελούν αντικείμενο ενεργού εκμετάλλευσης ισχύει όταν υποπίπτει στην αντίληψη του κατασκευαστή ενεργός εκμετάλλευση, ο κατασκευαστής δεν υποχρεούται να αναφέρει ευπάθειες οι οποίες είχαν ήδη υποπέσει στην αντίληψή του πριν από τις 11 Σεπτεμβρίου 2026 (ημερομηνία κατά την οποία αρχίζει να ισχύει η υποχρέωση αναφοράς). Ως εκ τούτου, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα δεν απαιτείται αναδρομική αναφορά τέτοιων ευπαθειών. Αντιθέτως, η υποχρέωση ισχύει όταν μια ευπάθεια υπέπεσε στην αντίληψη του κατασκευαστή πριν από τις 11 Σεπτεμβρίου 2026, χωρίς, ωστόσο, αυτός να γνωρίζει, κατά τον χρόνο εκείνο, καμία ενεργό εκμετάλλευσή της (είτε επειδή δεν είχε ακόμη λάβει χώρα είτε επειδή δεν είχε υποπέσει στην αντίληψη του κατασκευαστή). Εάν, μετά τις 11 Σεπτεμβρίου 2026, λάβει χώρα στη συνέχεια ενεργός εκμετάλλευση ή ενεργός εκμετάλλευση υποπέσει στην αντίληψη του κατασκευαστή, η ευπάθεια θεωρείται ότι αποτελεί αντικείμενο ενεργού εκμετάλλευσης και υπόκειται στην υποχρέωση αναφοράς.

218. Ομοίως, ο κατασκευαστής υποχρεούται μόνο να αναφέρει τις ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και περιέχονται στο προϊόν του με ψηφιακά στοιχεία. Όταν ένα προϊόν με ψηφιακά στοιχεία περιέχει ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και προέρχεται από δομοστοιχείο τρίτων, ο κατασκευαστής του προϊόντος με ψηφιακά στοιχεία υποχρεούται να γνωστοποιεί την εν λόγω ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης. Ωστόσο, εάν ένας κατασκευαστής γνωρίζει ότι δομοστοιχείο τρίτων περιέχει ευπάθεια, αλλά η εν λόγω ευπάθεια είτε i) δεν μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης στο προϊόν του με ψηφιακά στοιχεία (π.χ. επειδή ο ευπαθής κώδικας δεν είναι προσβάσιμος) είτε ii) δεν έχει αποτελέσει αντικείμενο εκμετάλλευσης στο προϊόν του με ψηφιακά στοιχεία, η εν λόγω ευπάθεια δεν μπορεί να χαρακτηριστεί ως ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και περιέχεται στο προϊόν του με ψηφιακά στοιχεία και, ως εκ τούτου, δεν υπόκειται σε υποχρεωτική αναφορά όσον αφορά τον εν λόγω κατασκευαστή. Ο εν λόγω κατασκευαστής εξακολουθεί να μπορεί να γνωστοποιήσει την εν λόγω ευπάθεια σε εθελοντική βάση, σύμφωνα με το άρθρο 15 του κανονισμού για την κυβερνοανθεκτικότητα. Απαιτείται επίσης η συμμόρφωση με τις απαιτήσεις χειρισμού ευπαθειών του παραρτήματος I μέρος II του κανονισμού για την κυβερνοανθεκτικότητα, καθώς και η αναφορά της ευπάθειας στο πρόσωπο ή την οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο, σύμφωνα με το άρθρο 13 παράγραφος 6 και όπως εξηγείται περαιτέρω στο τμήμα *9.2.1 Reporting upstream and sharing security fixes*.

([30]) Στον βαθμό που ο υποστηρικτής συμμετέχει στην ανάπτυξη προϊόντος με ψηφιακά στοιχεία.

219. Αφού αντιληφθούν ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή σοβαρό περιστατικό, οι κατασκευαστές υποχρεούνται επίσης, σύμφωνα με το άρθρο 14 παράγραφος 8, να ενημερώνουν τους επηρεαζόμενους χρήστες και, κατά περίπτωση, όλους τους χρήστες. Σε περίπτωση που δεν το πράξουν εγκαίρως, οι ΟΑΠΑΥ που έλαβαν την κοινοποίηση μπορούν να παρέχουν τις εν λόγω πληροφορίες στους χρήστες όταν αυτό θεωρείται αναλογικό και αναγκαίο για την πρόληψη ή τον μετριασμό των επιπτώσεων της εν λόγω ευπάθειας ή του περιστατικού.

220. Σύμφωνα με την προσέγγιση βάσει κινδύνων του κανονισμού για την κυβερνοανθεκτικότητα, η υποχρέωση ενημέρωσης των χρηστών που προβλέπεται στο άρθρο 14 παράγραφος 8 πρέπει να εφαρμόζεται με τρόπο αναλογικό και βάσει κινδύνων. Ειδικότερα, η παροχή πληροφοριών σχετικά με ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή σοβαρό περιστατικό δεν συνεπάγεται ότι οι πληροφορίες αυτές πρέπει να δημοσιοποιούνται ή να αποκαλύπτονται αδιακρίτως. Κατά περίπτωση και λαμβανομένων υπόψη της φύσης του προϊόντος με ψηφιακά στοιχεία, των επηρεαζόμενων χρηστών και του δυνητικού αντικτύπου της ευπάθειας ή του συμβάντος, οι κατασκευαστές μπορούν να περιορίζουν τη γνωστοποίηση λεπτομερών πληροφοριών στους σχετικούς ενδιαφερόμενους χρήστες ή πελάτες. Αυτό ισχύει ιδίως για τα προϊόντα με ψηφιακά στοιχεία που χρησιμοποιούνται σε ευαίσθητα ή ουσιώδη περιβάλλοντα, όπου η δημοσιοποίηση τεχνικών λεπτομερειών θα μπορούσε από μόνη της να αυξήσει τους κινδύνους κυβερνοασφάλειας ή να διευκολύνει την περαιτέρω εκμετάλλευση.

221. Μόλις αντιμετωπιστεί ή μετριαστεί επαρκώς η ευπάθεια, ενδέχεται να είναι σκόπιμη η ευρύτερη δημοσιοποίηση. Αυτό θα μπορούσε να ισχύει, για παράδειγμα, όταν η δημοσιοποίηση συμβάλλει στην αύξηση της γενικής ευαισθητοποίησης ή επιτρέπει στους χρήστες να επαληθεύουν ότι τα προϊόντα τους με ψηφιακά στοιχεία δεν επηρεάζονται πλέον. Στις περιπτώσεις αυτές, το επίπεδο λεπτομέρειας και η χρονική στιγμή κάθε ευρύτερης δημοσιοποίησης θα πρέπει να παραμένουν αναλογικά και να λαμβάνουν υπόψη τους υπολειπόμενους κινδύνους εκμετάλλευσης, τη φύση του προϊόντος με ψηφιακά στοιχεία και τα συμφέροντα των ενδιαφερόμενων χρηστών. Επιπλέον, βάσει του παραρτήματος I μέρος II σημείο 4 απαιτείται από τους κατασκευαστές να δημοσιοποιούν πληροφορίες σχετικά με τις διορθωμένες ευπάθειες μόλις καταστεί διαθέσιμη ενημέρωση ασφαλείας.

9.2. **Χειρισμός ευπαθειών**

9.2.1. *Αναφορά ανάντη και κοινοποίηση διορθώσεων ασφαλείας*

222. Βάσει του άρθρου 13 παράγραφος 6 του κανονισμού για την κυβερνοανθεκτικότητα, οι κατασκευαστές υποχρεούνται να αναφέρουν τις ευπάθειες των ενσωματωμένων δομοστοιχείων στο πρόσωπο ή στην οντότητα που κατασκευάζει ή συντηρεί το εν λόγω δομοστοιχείο (στο εξής: αναφορά ανάντη).

223. Οι κατασκευαστές υποχρεούνται να προβαίνουν σε αναφορά ανάντη μόνο όσον αφορά την έκδοση του δομοστοιχείου που ενσωματώνουν. Όταν το πρόσωπο ή η οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο έχει θεσπίσει πολιτικές ασφάλειας, συντονισμένες διαδικασίες γνωστοποίησης ευπαθειών ή καθορισμένους διαύλους για την αναφορά ευπαθειών, οι κατασκευαστές θα πρέπει να υποβάλλουν σχετικές αναφορές, ιδίως όταν η πρόωρη γνωστοποίηση μη διορθωμένων ευπαθειών μπορεί να αυξήσει τους κινδύνους για την κυβερνοασφάλεια. Επιπλέον, προκειμένου να μειωθεί η επιβάρυνση των ανάντη συντηρητών, ιδίως σε έργα ανοικτού κώδικα, οι κατασκευαστές δεν υποχρεούνται να προβαίνουν σε αναφορά ανάντη όταν μπορούν να επιβεβαιώσουν ότι το πρόσωπο ή η οντότητα που κατασκευάζει ή συντηρεί δομοστοιχείο γνωρίζει την ύπαρξη ευπάθειας. Οι κατασκευαστές ενθαρρύνονται να λαμβάνουν εύλογα μέτρα για την αποφυγή της υποβολής διπλών αναφορών, για παράδειγμα ελέγχοντας προσβάσιμες στο κοινό βάσεις δεδομένων ευπαθειών, ειδικές ανά έργο υποδείξεις ασφαλείας ή καθιερωμένα συστήματα παρακολούθησης προβλημάτων πριν από την πραγματοποίηση αναφοράς ανάντη.

224. Οι κατασκευαστές υποχρεούνται να αναφέρουν ανάντη μόνο τις ευπάθειες που υπάρχουν στο ίδιο το ενσωματωμένο δομοστοιχείο και όχι τις ευπάθειες που υπάρχουν ως αποτέλεσμα της σύνδεσης του δομοστοιχείου με άλλο κώδικα που έχει αναπτύξει ο κατασκευαστής ή της ενσωμάτωσης άλλων δομοστοιχείων. Ωστόσο, ενδέχεται να υπάρχουν περιπτώσεις στις οποίες η ενσωμάτωση δομοστοιχείου σε συγκεκριμένο προϊόν με ψηφιακά στοιχεία αποκαλύπτει ορισμένες συμπεριφορές, αλληλεπιδράσεις ή σχετικά με την ασφάλεια χαρακτηριστικά του εν λόγω δομοστοιχείου που δεν ήταν εμφανή ή δεν ήταν άμεσα αναγνωρίσιμα, μεμονωμένα. Στις περιπτώσεις αυτές, οι κατασκευαστές ενθαρρύνονται να κοινοποιούν τις πληροφορίες αυτές στο πρόσωπο ή στην οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο, προκειμένου να προωθούνται ορθές πρακτικές χειρισμού ευπαθειών που αποσκοπούν στη διευκόλυνση της αποτελεσματικής αποκατάστασης και στη βελτίωση της συνολικής ασφάλειας του οικοσυστήματος δομοστοιχείων.

225. Τέλος, οι κατασκευαστές δεν υποχρεούνται επίσης να προβαίνουν σε αναφορά της ευπάθειας ανάντη, όταν το δομοστοιχείο δεν διαθέτει πλέον συντηρητή ή όταν ο κατασκευαστής δεν βασίζεται πλέον στον αρχικό συντηρητή για νέες εκδόσεις ή επιδιορθώσεις ασφαλείας. Ωστόσο, στις περιπτώσεις αυτές, ο κατασκευαστής ενθαρρύνεται να ενημερώνει τους χρήστες για το εν λόγω δομοστοιχείο μέσω εύλογων εναλλακτικών μέτρων, π.χ. μέσω υφιστάμενων μηχανισμών «κοινότητας» (όπως κατάλογοι διευθύνσεων ή δελτία προβλημάτων) ή μέσω δημόσιων αρχείων ευπαθειών.

226. Επιπλέον, σύμφωνα με το άρθρο 13 παράγραφος 6, οι κατασκευαστές που έχουν αναπτύξει τροποποίηση λογισμικού για την αντιμετώπιση ευπάθειας σε ενσωματωμένο δομοστοιχείο υποχρεούνται να κοινοποιούν την εν λόγω τροποποίηση λογισμικού (στο εξής: διόρθωση ασφαλείας) στο πρόσωπο ή στην οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο (στο εξής: κοινοποίηση ανάντη).

227. Όταν οι κατασκευαστές υποχρεούνται να κοινοποιήσουν διόρθωση ασφάλειας σύμφωνα με το άρθρο 13 παράγραφος 6, η διόρθωση θα πρέπει, κατά περίπτωση, να παρέχεται σε μηχαναγνώσιμο μορφότυπο, με τρόπο που να μπορεί εύκολα να επαληθευτεί και, κατά περίπτωση, να ενσωματωθεί από το πρόσωπο ή την οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο. Όταν το δομοστοιχείο είναι ελεύθερο δομοστοιχείο ανοικτού κώδικα, η διόρθωση ασφαλείας θα πρέπει να κοινοποιείται με τρόπο συμβατό με την άδεια του εν λόγω δομοστοιχείου, για παράδειγμα μέσω κοινοποίησης βάσει της ίδιας άδειας ή βάσει άδειας που επιτρέπει στον συντηρητή να διανέμει τη διόρθωση ασφαλείας βάσει της δικής του άδειας. Όταν ο συντηρητής του εν λόγω δομοστοιχείου διαθέτει κατευθυντήριες γραμμές σχετικά με τον τρόπο κοινοποίησης των διορθώσεων ασφαλείας, ο κατασκευαστής θα πρέπει να ακολουθεί τις εν λόγω κατευθυντήριες γραμμές.

228. Ωστόσο, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα δεν απαιτείται από τους κατασκευαστές να διασφαλίζουν ότι οι διορθώσεις ασφαλείας τους γίνονται κατ' ανάγκη αποδεκτές από το πρόσωπο ή την οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο. Επίσης, δεν υποχρεούνται να διασφαλίζουν ότι οι εν λόγω διορθώσεις είναι κατ' ανάγκη ενσωματωμένες στο αποθετήριο κωδίκων του δομοστοιχείου, για παράδειγμα όταν ο συντηρητής μπορεί να προτιμήσει διαφορετική επιλογή για την επίλυση του προβλήματος. Ομοίως, οι κατασκευαστές δεν υποχρεούνται να αποδέχονται προτεινόμενη διόρθωση που έχει αναπτυχθεί από τον συντηρητή του δομοστοιχείου και μπορούν να επιλέξουν να μετριάσουν το πρόβλημα με άλλους κατάλληλους τρόπους.

229. Σε ορισμένες περιπτώσεις, το πρόσωπο ή η οντότητα που κατασκευάζει ή συντηρεί το δομοστοιχείο μπορεί να έχει ήδη παράσχει διόρθωση ασφαλείας για την αντιμετώπιση της ευπάθειας, αλλά ο κατασκευαστής μπορεί να εφαρμόζει διαφορετική στρατηγική μετριασμού (για παράδειγμα, αλλάζοντας διαφορετική διαμόρφωση). Στις περιπτώσεις αυτές, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα, δεν απαιτείται από τον κατασκευαστή να κοινοποιεί την τροποποίηση άλλου εξαρτήματος του συστήματος ανάντη. Ωστόσο, ο κατασκευαστής ενθαρρύνεται να το πράττει, όταν με αυτόν τον τρόπο μπορεί να υποστηρίξει το πρόσωπο ή την οντότητα που συντηρεί το δομοστοιχείο.

9.2.2. *Γνωστές εκμεταλλεύσιμες ευπάθειες*

230. Μία από τις ουσιώδεις απαιτήσεις του παραρτήματος I μέρος I του κανονισμού για την κυβερνοανθεκτικότητα προβλέπει ότι, με βάση την εκτίμηση κινδύνων για την κυβερνοασφάλεια που αναφέρεται στο άρθρο 13 παράγραφος 2 και κατά περίπτωση, τα προϊόντα με ψηφιακά στοιχεία πρέπει να διατίθενται στην αγορά χωρίς γνωστές εκμεταλλεύσιμες ευπάθειες.

231. Στο άρθρο 3 σημείο 41), ως «εκμεταλλεύσιμη ευπάθεια» ορίζεται η «ευπάθεια που θα μπορούσε να χρησιμοποιηθεί αποτελεσματικά από αντίπαλο υπό πρακτικές συνθήκες λειτουργίας». Δεν είναι όλες οι ευπάθειες εκμεταλλεύσιμες υπό πρακτικές συνθήκες λειτουργίας και ορισμένες ευπάθειες μπορούν να αποτελέσουν αντικείμενο εκμετάλλευσης μόνο υπό θεωρητικές συνθήκες (π.χ. σε εργαστήριο ή σε προσομοίωση) και/ή όχι υπό συνθήκες που θα προέκυπταν στο επιχειρησιακό περιβάλλον προϊόντος με ψηφιακά στοιχεία.

232. Σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα, απαιτείται από τους κατασκευαστές να διαθέτουν κατάλληλες πολιτικές και διαδικασίες για τον χειρισμό και την αποκατάσταση πιθανών ευπαθειών που αναφέρονται από εσωτερικές ή εξωτερικές πηγές (άρθρο 13 παράγραφος 8). Ωστόσο, δεν προσδιορίζεται ρητά πότε μια εκμεταλλεύσιμη ευπάθεια θα πρέπει να θεωρείται ότι έχει υποπέσει στην αντίληψη του κατασκευαστή, με αποτέλεσμα να ενεργοποιείται η υποχρέωση συμμόρφωσης με την εν λόγω ουσιώδη απαίτηση κατά τη στιγμή της θέσης σε κυκλοφορία στην αγορά.

233. Μια ευπάθεια θα πρέπει να θεωρείται γνωστή όταν περιλαμβάνεται σε σχετικές δημόσια προσβάσιμες βάσεις δεδομένων ευπαθειών, όπως η ευρωπαϊκή βάση δεδομένων ευπαθειών που θεσπίστηκε με το άρθρο 12 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555 ή άλλες σημαντικές βάσεις δεδομένων ευπαθειών.

234. Επιπλέον, μια ευπάθεια μπορεί επίσης να είναι γνωστή όταν ο κατασκευαστής έχει ενημερωθεί σχετικά μέσω μη δημόσιων πληροφοριών, για παράδειγμα μέσω συντονισμένης γνωστοποίησης από ερευνητή στον τομέα της ασφάλειας ή μέσω εσωτερικών δοκιμών και αναλύσεων του ίδιου του κατασκευαστή, μεταξύ άλλων, για παράδειγμα, με τη χρήση υπηρεσιών που βασίζονται στην ΤΝ. Ομοίως, μια ευπάθεια μπορεί να είναι γνωστή όταν έχει δημοσιοποιηθεί δημοσίως και σε περίοπτη θέση σε αξιόπιστα μέσα ενημέρωσης, συμπεριλαμβανομένων εξειδικευμένων δημοσιεύσεων για την κυβερνοασφάλεια ή γενικών μέσων μαζικής ενημέρωσης.

235. Ωστόσο, το γεγονός ότι αναφέρεται ή διαπιστώνεται μια ευπάθεια δεν σημαίνει, από μόνο του, ότι είναι εκμεταλλεύσιμη στην πράξη ή μπορεί να εφαρμοστεί στο συγκεκριμένο προϊόν με ψηφιακά στοιχεία. Ο κατασκευαστής θα πρέπει να διερευνά και να επιβεβαιώνει την ακρίβεια των εν λόγω πληροφοριών, καθώς και τη δυνατότητα εφαρμογής στο δικό του προϊόν με ψηφιακά στοιχεία. Ως εκ τούτου, μπορεί να μεσολαβήσει περιορισμένο χρονικό διάστημα μεταξύ της πρώτης αναφοράς της ευπάθειας και της επιβεβαίωσής της. Όπως αναφέρεται στο τμήμα *9.1 Reporting obligations*, θα πρέπει να δίνεται έμφαση στην άμεση ανάληψη δράσης για τη διερεύνηση και την αντίδραση.

236. Επιπλέον, η υποχρέωση των κατασκευαστών να συμμορφώνονται με τις ουσιώδεις απαιτήσεις που ορίζονται στο παράρτημα Ι μέρος Ι ισχύει κατά τη στιγμή της θέσης σε κυκλοφορία στην αγορά, σύμφωνα με το άρθρο 13 παράγραφος 1. Στην πράξη, ενδέχεται να ανακαλυφθούν νέες πιθανές εκμεταλλεύσιμες ευπάθειες κατά τα τελικά στάδια του κύκλου ανάπτυξης του προϊόντος με ψηφιακά στοιχεία, μεταξύ άλλων λίγο πριν από την είσοδό του στην αλυσίδα διανομής (και, ως εκ τούτου, της θέσης του σε κυκλοφορία στην αγορά).

237. Δεδομένου ότι η υποχρέωση θέσης προϊόντων με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά χωρίς γνωστές εκμεταλλεύσιμες ευπάθειες αποτελεί υποχρέωση βάσει κινδύνων, εναπόκειται στον κατασκευαστή να καθορίσει αν, με βάση την εκτίμηση κινδύνων κυβερνοασφάλειας, το προϊόν με ψηφιακά στοιχεία μπορεί να τεθεί με ασφάλεια σε κυκλοφορία στην αγορά, σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα. Εναλλακτικά, ο κατασκευαστής μπορεί να αποφασίσει ότι μια ευπάθεια που ενδέχεται να έχει καταστεί γνωστή πρέπει να διορθωθεί πριν από τη θέση του προϊόντος με ψηφιακά στοιχεία σε κυκλοφορία στην αγορά. Στο πλαίσιο λήψης της εν λόγω απόφασης, οι κατασκευαστές θα πρέπει να λαμβάνουν υπόψη τη σοβαρότητα, την εκμεταλλευσιμότητα και τον δυνητικό αντίκτυπο της ευπάθειας, καθώς και τους κινδύνους που προκύπτουν για το ίδιο το προϊόν με ψηφιακά στοιχεία κατά τη χρήση του. Μπορούν επίσης να λαμβάνουν υπόψη τους κινδύνους που προκύπτουν από την αναβολή της διάθεσης του προϊόντος έως ότου διορθωθεί η ευπάθεια, για παράδειγμα επειδή η νέα διάθεση αντιμετωπίζει επίσης άλλες εκμεταλλεύσιμες ευπάθειες ή είναι αναγκαία για τη συνέχιση της λειτουργίας κρίσιμων συστημάτων. Σε κάθε περίπτωση, μόλις ένα προϊόν με ψηφιακά στοιχεία τεθεί σε κυκλοφορία στην αγορά, ο κατασκευαστής εξακολουθεί να υπόκειται στην υποχρέωση αποτελεσματικού χειρισμού των ευπαθειών σύμφωνα με τις απαιτήσεις χειρισμού ευπαθειών που ορίζονται στο παράρτημα Ι μέρος ΙΙ.

9.2.3. *Αποτελεσματικές και τακτικές δοκιμές και αξιολογήσεις*

238. Βάσει του παραρτήματος Ι μέρος ΙΙ σημείο 3 απαιτείται από τους κατασκευαστές να εφαρμόζουν αποτελεσματικές και τακτικές δοκιμές και αξιολογήσεις του προϊόντος με ψηφιακά στοιχεία καθ' όλη τη διάρκεια της περιόδου υποστήριξής του. Για την εφαρμογή τακτικών δοκιμών δεν απαιτείται η μηχανική επανάληψη, σε καθορισμένα χρονικά διαστήματα, μιας αμετάβλητης διαδικασίας δοκιμών. Συνεπάγεται την τακτική αξιολόγηση του αν υπάρχουν νέα στοιχεία, όπως απειλές που εντοπίστηκαν πρόσφατα ή ευπάθειες που ανακαλύφθηκαν πρόσφατα, βάσει των οποίων απαιτείται η επικαιροποίηση των υφιστάμενων δοκιμών, και την ανάλογη εκτέλεση των δοκιμών.

239. Η συχνότητα, το βάθος και το περιεχόμενο της αξιολόγησης θα πρέπει να είναι αναλογικά προς το προφίλ κινδύνου κυβερνοασφάλειας του προϊόντος με ψηφιακά στοιχεία, την εξέλιξή του σε βάθος χρόνου και την κατάσταση του τοπίου των απειλών. Όταν η αξιολόγηση εντοπίζει συναφή νέα στοιχεία που επηρεάζουν το σύνολο δοκιμών, θα πρέπει να σχεδιάζονται και να εκτελούνται νέες ή τροποποιημένες δοκιμές στο προϊόν, ώστε να διασφαλίζεται ότι δεν παραμένουν ανεπίλυτες οι ευπάθειες. Σε αυτό το πλαίσιο, μπορεί να απαιτείται η εκ νέου εκτέλεση υφιστάμενων δοκιμών, όταν η τροποποίηση του προϊόντος με ψηφιακά στοιχεία καθιστά κατάλληλους αυτούς τους τύπους δοκιμών, όπως οι δοκιμές παλινδρόμησης.

240. Όταν κατά την αξιολόγηση δεν εντοπίζονται τέτοια στοιχεία, δεν χρειάζεται να σχεδιαστούν πρόσθετες δοκιμές. Άλλες υποχρεώσεις χειρισμού ευπαθειών, συμπεριλαμβανομένης της υποχρέωσης αντιμετώπισης και αποκατάστασης ευπαθειών σε σχέση με τους κινδύνους που προκύπτουν, εξακολουθούν να ισχύουν παράλληλα.

9.3. **Αλληλεπίδραση με άλλη νομοθεσία**

9.3.1. *Κανονισμός (ΕΕ) 2019/2144 και κανονισμός (ΕΕ) αριθ. 168/2013*

241. Το άρθρο 2 παράγραφος 2 στοιχείο γ) του κανονισμού για την κυβερνοανθεκτικότητα ορίζει ότι ο κανονισμός δεν εφαρμόζεται σε προϊόντα με ψηφιακά στοιχεία στα οποία εφαρμόζεται ο κανονισμός (ΕΕ) 2019/2144. Ο κανονισμός (ΕΕ) 2019/2144 ισχύει για τα «οχήματα των κατηγοριών M, N και O», όπως ορίζονται στο άρθρο 4 του κανονισμού (ΕΕ) 2018/858 και για τα συστήματα, τα κατασκευαστικά στοιχεία και τις χωριστές τεχνικές μονάδες που σχεδιάζονται και κατασκευάζονται για τα εν λόγω οχήματα».

242. Ομοίως, τα προϊόντα με ψηφιακά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) αριθ. 168/2013 έχουν εξαιρεθεί από το πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα με τον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2025/1535 της Επιτροπής. Ο κανονισμός (ΕΕ) αριθ. 168/2013 ισχύει για τα οχήματα της κατηγορίας L και «για τις περιπτώσεις των συστημάτων, των μηχανικών μερών και των χωριστών τεχνικών μονάδων, καθώς και των μερών και των εξαρτημάτων, που σχεδιάστηκαν και κατασκευάστηκαν για τα εν λόγω οχήματα» (άρθρο 2 παράγραφος 1).

243. Τα οχήματα για τα οποία ισχύουν οι εν λόγω κανονισμοί δεν υπόκεινται στον κανονισμό για την κυβερνοανθεκτικότητα. Επιπλέον, απαιτούνται πρόσθετες διευκρινίσεις όσον αφορά το πεδίο εφαρμογής της εξαίρεσης για τα συστήματα, τα κατασκευαστικά στοιχεία, τις χωριστές τεχνικές μονάδες, τα εξαρτήματα και τον εξοπλισμό (για τους σκοπούς του παρόντος τμήματος, στο εξής: δομοστοιχεία) που σχεδιάζονται και κατασκευάζονται για τα εν λόγω οχήματα, τα οποία θεωρούνται προϊόντα με ψηφιακά στοιχεία κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα.

244. Θεωρείται ότι τα εν λόγω κατασκευαστικά στοιχεία δεν υπόκεινται στον κανονισμό για την κυβερνοανθεκτικότητα, υπό την προϋπόθεση ότι σχεδιάζονται και κατασκευάζονται αποκλειστικά για ενσωμάτωση σε οχήματα που καλύπτονται από τους κανονισμούς (ΕΕ) 2019/2144 και (ΕΕ) αριθ. 168/2013. Αυτό ισχύει ανεξάρτητα από το αν ο κατασκευαστής του εν λόγω δομοστοιχείου το πωλεί απευθείας στον κατασκευαστή του οχήματος ή σε άλλον οικονομικό φορέα στην αλυσίδα εφοδιασμού της αυτοκινητοβιομηχανίας, εφόσον το δομοστοιχείο προορίζεται σαφώς και είναι κατάλληλο μόνο για τελική ενσωμάτωση στα εν λόγω οχήματα.

245. Αντιθέτως, ένας κατασκευαστής που πωλεί γενικά δομοστοιχεία τα οποία είναι προϊόντα με ψηφιακά στοιχεία που μπορούν να ενσωματωθούν σε διαφορετικούς τύπους προϊόντων και όχι αποκλειστικά σε οχήματα που καλύπτονται από τους εν λόγω κανονισμούς, υπόκειται στον κανονισμό για την κυβερνοανθεκτικότητα.

246. Η αξιολόγηση του αν ένα δομοστοιχείο τίθεται σε κυκλοφορία στην αγορά κατά την έννοια του κανονισμού για την κυβερνοανθεκτικότητα πρέπει να βασίζεται στις αντικειμενικές συνθήκες υπό τις οποίες διατίθεται στην αγορά. Όταν ένας κατασκευαστής προσφέρει ένα δομοστοιχείο που δεν είναι αποκλειστικά κατάλληλο για τελική ενσωμάτωση εντός των εν λόγω οχημάτων μέσω διαύλων διανομής που είναι ανοικτοί σε πελάτες εκτός της αλυσίδας εφοδιασμού της αυτοκινητοβιομηχανίας, όπως καταστήματα γενικού εμπορίου ή διαδικτυακοί δίαυλοι πωλήσεων που δέχονται παραγγελίες από το ευρύ κοινό, το εν λόγω δομοστοιχείο εμπίπτει στο πεδίο εφαρμογής του κανονισμού για την κυβερνοανθεκτικότητα, ανεξάρτητα από τυχόν δηλώσεις σχετικά με τη σκοπούμενη χρήση του. Στις περιπτώσεις αυτές, το δομοστοιχείο δεν μπορεί να θεωρηθεί ότι έχει σχεδιαστεί και κατασκευαστεί αποκλειστικά για ενσωμάτωση σε οχήματα που καλύπτονται από τους κανονισμούς (ΕΕ) 2019/2144 και (ΕΕ) αριθ. 168/2013 και ο κατασκευαστής υποχρεούται να συμμορφώνεται με τον κανονισμό για την κυβερνοανθεκτικότητα. Αντιθέτως, η χρήση περιορισμένων διαύλων διανομής μεταξύ επιχειρήσεων που περιορίζονται στην αλυσίδα εφοδιασμού της αυτοκινητοβιομηχανίας μπορεί να υποδηλώνει ότι έχει σχεδιαστεί και κατασκευαστεί αποκλειστικά για την εν λόγω ενσωμάτωση.

9.3.2. *Ισχύς των πιστοποιητικών εξέτασης τύπου ΕΕ (άρθρο 69 παράγραφος 1)*

247. Στο άρθρο 69 παράγραφος 1 του κανονισμού για την κυβερνοανθεκτικότητα αναφέρεται ότι «Τα πιστοποιητικά εξέτασης τύπου ΕΕ και οι αποφάσεις έγκρισης που εκδίδονται σχετικά με τις απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία που υπόκεινται σε άλλη ενωσιακή νομοθεσία εναρμόνισης πέραν του παρόντος κανονισμού παραμένουν σε ισχύ έως τις 11 Ιουνίου 2028, εκτός εάν λήγουν πριν από την εν λόγω ημερομηνία, ή εκτός εάν ορίζεται διαφορετικά στην εν λόγω άλλη ενωσιακή νομοθεσία εναρμόνισης, οπότε εξακολουθούν να ισχύουν όπως αναφέρεται στην εν λόγω νομοθεσία».

248. Η συνεχιζόμενη ισχύς των εν λόγω πιστοποιητικών και αποφάσεων έγκρισης θα πρέπει να θεωρείται ότι περιορίζεται στους κινδύνους κυβερνοασφάλειας και στις αντίστοιχες απαιτήσεις που καλύπτονται από την αντίστοιχη ενωσιακή νομοθεσία εναρμόνισης βάσει της οποίας εκδόθηκαν. Όσον αφορά τους εν λόγω κινδύνους, οι κατασκευαστές δεν υποχρεούνται να επαναξιολογούν ή να αποδεικνύουν εκ νέου τη συμμόρφωση αποκλειστικά για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα κατά τη διάρκεια της περιόδου ισχύος που αναφέρεται στο άρθρο 69 παράγραφος 1 για προϊόντα με ψηφιακά στοιχεία που προτίθενται να θέσουν σε κυκλοφορία στην αγορά από την 11η Δεκεμβρίου 2027 ή μεταγενέστερα και έως την 11η Ιουνίου 2028 ([31]). Αυτό ισχύει για τα πιστοποιητικά και τις αποφάσεις έγκρισης που εκδίδονται όταν η ισχύουσα ενωσιακή νομοθεσία εναρμόνισης απαιτεί από τον κατασκευαστή να διενεργεί τη διαδικασία αξιολόγησης της συμμόρφωσης μέσω κοινοποιημένου οργανισμού, καθώς και όταν ο κατασκευαστής έχει επιλέξει οικειοθελώς να το πράξει.

249. Κατά συνέπεια, η ύπαρξη έγκυρου πιστοποιητικού ή απόφασης έγκρισης βάσει άλλης ενωσιακής νομοθεσίας εναρμόνισης δεν απαλλάσσει τους κατασκευαστές από την υποχρέωση διενέργειας ολοκληρωμένης εκτίμησης κινδύνων για την κυβερνοασφάλεια στο πλαίσιο του κανονισμού για την κυβερνοανθεκτικότητα (ή από άλλες υποχρεώσεις που απορρέουν από αυτήν). Αντ' αυτού, τους επιτρέπει να βασίζονται σε υφιστάμενες πιστοποιήσεις ως αποδεικτικά στοιχεία συμμόρφωσης για τη διαδικασία αξιολόγησης της συμμόρφωσης, στον βαθμό που οι αντίστοιχοι κίνδυνοι κυβερνοασφάλειας καλύπτονται ήδη. Όταν το πιστοποιητικό ή η απόφαση έγκρισης έχει ισχύ βάσει άλλης ενωσιακής νομοθεσίας εναρμόνισης που εκτείνεται πέραν της 11ης Ιουνίου 2028, ο κατασκευαστής μπορεί, ωστόσο, να βασιστεί στο εν λόγω πιστοποιητικό ή στην εν λόγω απόφαση για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα μόνο έως τις 11 Ιουνίου 2028.

250. Όταν η εκτίμηση κινδύνων για την κυβερνοασφάλεια που διενεργείται σύμφωνα με το άρθρο 13 παράγραφος 2 εντοπίζει πρόσθετους κινδύνους που δεν καλύπτονται από τις απαιτήσεις κυβερνοασφάλειας στις οποίες βασίζεται το υφιστάμενο πιστοποιητικό ή η απόφαση έγκρισης, οι κατασκευαστές παραμένουν υπεύθυνοι για την αντιμετώπιση των εν λόγω κινδύνων σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα. Στις περιπτώσεις αυτές, η συμμόρφωση απαιτεί να αξιολογούνται και να μετριάζονται τα κενά που εντοπίζονται, ανεξάρτητα από τη συνέχιση της ισχύος του υφιστάμενου πιστοποιητικού ή της απόφασης έγκρισης.

251. Ως παράδειγμα μπορεί να αναφερθεί η περίπτωση κατά την οποία ένα προϊόν με ψηφιακά στοιχεία υπόκειται στις απαιτήσεις κυβερνοασφάλειας που ορίζονται στον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2022/30 της Επιτροπής για τη συμπλήρωση της οδηγίας 2014/53/ΕΕ [κατ' εξουσιοδότηση πράξη σχετικά με την οδηγία για τον ραδιοεξοπλισμό (RED)] και για το οποίο έχει εκδοθεί πιστοποιητικό εξέτασης τύπου ΕΕ ή απόφαση έγκρισης βάσει των εν λόγω απαιτήσεων. Στην περίπτωση αυτήν, το πιστοποιητικό ή η απόφαση παραμένει σε ισχύ, σύμφωνα με το άρθρο 69 παράγραφος 1, για τους κινδύνους κυβερνοασφάλειας που καλύπτονται από το εν λόγω πιστοποιητικό και σχετίζονται με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας της οδηγίας 2014/53/ΕΕ (στο εξής: «οδηγία για τον ραδιοεξοπλισμό» ή «RED»).

252. Στις περιπτώσεις αυτές, οι κατασκευαστές δεν υποχρεούνται, για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα, να επαναξιολογήσουν ή να αποδείξουν εκ νέου τη συμμόρφωση όσον αφορά τους κινδύνους που έχουν ήδη αντιμετωπιστεί με τα εν λόγω πιστοποιητικά, για όσο διάστημα το σχετικό πιστοποιητικό ή η απόφαση έγκρισης παραμένει σε ισχύ και, σε κάθε περίπτωση, όχι πέραν της 11ης Ιουνίου 2028. Σε αυτό το πλαίσιο περιλαμβάνονται, για παράδειγμα, κίνδυνοι κυβερνοασφάλειας που σχετίζονται με την προστασία δικτύου, την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής ή την πρόληψη της απάτης (στον βαθμό που οι εν λόγω κίνδυνοι καλύπτονται από το εν λόγω πιστοποιητικό) και οι οποίοι συνδέονται με τις απαιτήσεις κυβερνοασφάλειας της οδηγίας για τον ραδιοεξοπλισμό και αντικατοπτρίζονται στην αξιολόγηση της συμμόρφωσης.

253. Ωστόσο, όταν η εκτίμηση κινδύνων για την κυβερνοασφάλεια που διενεργείται σύμφωνα με το άρθρο 13 παράγραφος 2 του κανονισμού για την κυβερνοανθεκτικότητα εντοπίζει πρόσθετους κινδύνους για την κυβερνοασφάλεια που δεν καλύπτονται από τα εν λόγω πιστοποιητικά, οι κατασκευαστές παραμένουν υπεύθυνοι για την αντιμετώπιση των εν λόγω κινδύνων σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα. Στους εν λόγω κινδύνους μπορεί να περιλαμβάνονται, για παράδειγμα, κίνδυνοι που σχετίζονται με τις διαδικασίες χειρισμού ευπαθειών, την ελαχιστοποίηση των δεδομένων και τον περιορισμό της επιφάνειας επίθεσης ή άλλες ειδικές ανά προϊόν πτυχές κυβερνοασφάλειας που δεν καλύπτονται από τα εν λόγω πιστοποιητικά ή, σε κάθε περίπτωση, δεν καλύπτονται από τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας της οδηγίας για τον ραδιοεξοπλισμό.

254. Ως εκ τούτου, η ύπαρξη έγκυρου πιστοποιητικού εξέτασης τύπου ΕΕ ή απόφασης έγκρισης βάσει της οδηγίας για τον ραδιοεξοπλισμό για τις βασικές απαιτήσεις της σχετικά με την κυβερνοασφάλεια δεν αποδεικνύει, αφ' εαυτής, πλήρη συμμόρφωση με τον κανονισμό για την κυβερνοανθεκτικότητα. Αντ' αυτού, επιτρέπει στους κατασκευαστές να βασίζονται στο εν λόγω πιστοποιητικό ή απόφαση ως απόδειξη της συμμόρφωσης για τους αντίστοιχους κινδύνους, διασφαλίζοντας παράλληλα ότι τυχόν υπολειπόμενοι ή πρόσφατα εντοπισθέντες κίνδυνοι αξιολογούνται και μετριάζονται σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα.

([31]) Τα προϊόντα με ψηφιακά στοιχεία που τίθενται σε κυκλοφορία στην αγορά πριν από τις 11 Δεκεμβρίου 2027 υπόκεινται στην ενωσιακή νομοθεσία που ισχύει κατά τον χρόνο της θέσης τους σε κυκλοφορία στην αγορά και, εφόσον συμμορφώνονται, μπορούν να πωλούνται και να τίθενται σε λειτουργία, εκτός εάν, από τις 11 Δεκεμβρίου 2027 και μετά, υποστούν ουσιαστικές τροποποιήσεις. Για τις έννοιες της «θέσης σε κυκλοφορία στην αγορά» και της «διάθεσης στην αγορά», βλ. επίσης τμήμα *2.1 Placing on the market* του παρόντος εγγράφου, καθώς και κεφάλαιο 2 του Γαλάζιου Οδηγού.

255. Ομοίως, όταν ένα προϊόν με ψηφιακά στοιχεία υπόκειται στις βασικές απαιτήσεις υγείας και ασφάλειας που σχετίζονται με την κυβερνοασφάλεια οι οποίες ορίζονται στον κανονισμό (ΕΕ) 2023/1230 (κανονισμός για τα μηχανήματα), ο οποίος εφαρμόζεται πλήρως από τις 20 Ιανουαρίου 2027, και όταν έχει εκδοθεί πιστοποιητικό εξέτασης τύπου ΕΕ ή απόφαση έγκρισης βάσει των εν λόγω απαιτήσεων, το εν λόγω πιστοποιητικό ή η εν λόγω απόφαση έγκρισης εξακολουθεί να ισχύει, σύμφωνα με το άρθρο 69 παράγραφος 1 του κανονισμού για την κυβερνοανθεκτικότητα, για τους κινδύνους κυβερνοασφάλειας που καλύπτονται από τον κανονισμό για τα μηχανήματα.

256. Ειδικότερα, τα ανωτέρω αφορούν πτυχές κυβερνοασφάλειας που σχετίζονται με την προστασία από αλλοίωση και την ασφάλεια και αξιοπιστία των συστημάτων χειρισμού, όπως καθορίζονται στα σημεία 1.1.9 και 1.2.1 του παραρτήματος III του κανονισμού για τα μηχανήματα. Όσον αφορά τους κινδύνους αυτούς, οι κατασκευαστές δεν υποχρεούνται, για τους σκοπούς του κανονισμού για την κυβερνοανθεκτικότητα, να επαναξιολογούν ή να αποδεικνύουν εκ νέου τη συμμόρφωση για όσο διάστημα το σχετικό πιστοποιητικό ή η σχετική απόφαση έγκρισης παραμένει σε ισχύ και, σε κάθε περίπτωση, όχι πέραν της 11ης Ιουνίου 2028. Αυτό ισχύει στον βαθμό που οι εν λόγω κίνδυνοι έχουν αντιμετωπιστεί στο πλαίσιο της αξιολόγησης της συμμόρφωσης βάσει του κανονισμού για τα μηχανήματα.

257. Όπως και με τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας της οδηγίας για τον ραδιοεξοπλισμό που αναφέρονται ανωτέρω, όταν η εκτίμηση κινδύνων κυβερνοασφάλειας που διενεργείται σύμφωνα με το άρθρο 13 παράγραφος 2 του κανονισμού για την κυβερνοανθεκτικότητα εντοπίζει πρόσθετους κινδύνους κυβερνοασφάλειας που δεν καλύπτονται από το σχετικό πιστοποιητικό που εκδίδεται σύμφωνα με τον κανονισμό για τα μηχανήματα και σχετίζονται με τις απαιτήσεις κυβερνοασφάλειας του εν λόγω κανονισμού, οι κατασκευαστές παραμένουν υπεύθυνοι για την αντιμετώπιση των εν λόγω κινδύνων σύμφωνα με τον κανονισμό για την κυβερνοανθεκτικότητα.